

## SOA-C02 Dumps

### AWS Certified SysOps Administrator - Associate (SOA-C02)

<https://www.certleader.com/SOA-C02-dumps.html>



**NEW QUESTION 1**

- (Exam Topic 1)

A company updates its security policy to prohibit the public exposure of any data in Amazon S3 buckets in the company's account. What should a SysOps administrator do to meet this requirement?

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

**Answer:** A

**Explanation:**

Using Amazon S3 Block Public Access

as a centralized way to limit public access. Block Public Access

settings override bucket policies and object permissions. Be sure to enable Block Public Access for all accounts and buckets that you don't want publicly accessible.

<https://aws.amazon.com/premiumsupport/knowledge-center/secure-s3-resources/#:~:text=Using%20Amazon%2>

**NEW QUESTION 2**

- (Exam Topic 1)

An application team uses an Amazon Aurora MySQL DB cluster with one Aurora Replica. The application team notices that the application read performance degrades when user connections exceed 200. The number of user connections is typically consistent around 180, with occasional sudden increases above 200 connections. The application team wants the application to automatically scale as user demand increases or decreases.

Which solution will meet these requirements?

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

**Answer:** C

**NEW QUESTION 3**

- (Exam Topic 1)

A company has created a NAT gateway in a public subnet in a VPC. The VPC also contains a private subnet that includes Amazon EC2 instances. The EC2 instances use the NAT gateway to access the internet to download patches and updates. The company has configured a VPC flow log for the elastic network interface of the NAT gateway. The company is publishing the output to Amazon CloudWatch Logs.

A SysOps administrator must identify the top five internet destinations that the EC2 instances in the private subnet communicate with for downloads.

What should the SysOps administrator do to meet this requirement in the MOST operationally efficient way?

- A. Use AWS CloudTrail Insights events to identify the top five internet destinations.
- B. Use Amazon CloudFront standard logs (access logs) to identify the top five internet destinations.
- C. Use CloudWatch Logs Insights to identify the top five internet destinations.
- D. Change the flow log to publish logs to Amazon S3. Use Amazon Athena to query the log files in Amazon S3.

**Answer:** C

**NEW QUESTION 4**

- (Exam Topic 1)

A SysOps administrator noticed that the cache hit ratio for an Amazon CloudFront distribution is less than 10%.

Which collection of configuration changes will increase the cache hit ratio for the distribution? (Select TWO.)

- A. Ensure that only required cookies, query strings, and headers are forwarded in the Cache Behavior Settings.
- B. Change the Viewer Protocol Policy to use HTTPS only.
- C. Configure the distribution to use presigned cookies and URLs to restrict access to the distribution.
- D. Enable automatic compression of objects in the Cache Behavior Settings.
- E. Increase the CloudFront time to live (TTL) settings in the Cache Behavior Settings.

**Answer:** AE

**Explanation:**

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cache-hit-ratio.html#cache-hit-ratio-ht>

**NEW QUESTION 5**

- (Exam Topic 1)

A company wants to track its AWS costs in all member accounts that are part of an organization in AWS Organizations. Managers of the member accounts want to receive a notification when the estimated costs exceed a predetermined amount each month. The managers are unable to configure a billing alarm. The IAM permissions for all users are correct. What could be the cause of this issue?

- A. The management/payer account does not have billing alerts turned on.
- B. The company has not configured AWS Resource Access Manager (AWS RAM) to share billing information between the member accounts and the management/payer account.
- C. Amazon GuardDuty is turned on for all the accounts.
- D. The company has not configured an AWS Config rule to monitor billing.

**Answer: B**

**NEW QUESTION 6**

- (Exam Topic 1)

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

**Answer: A**

**NEW QUESTION 7**

- (Exam Topic 1)

A SysOps administrator receives an alert from Amazon GuardDuty about suspicious network activity on an Amazon EC2 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
- B. Assign the new security group to the EC2 instance
- C. Use VPC flow logs with Amazon Athena to block traffic to the external IP address
- D. Create a network ACL. Add an outbound deny rule for traffic to the external IP address
- E. Create a new security group to block traffic to the external IP address. Assign the new security group to the entire VPC

**Answer: A**

**NEW QUESTION 8**

- (Exam Topic 1)

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

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

**Answer: C**

**NEW QUESTION 9**

- (Exam Topic 1)

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 Multi-AZ 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? (Select 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

**Answer: AD**

**NEW QUESTION 10**

- (Exam Topic 1)

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

**Answer: D**

**Explanation:**

<https://docs.aws.amazon.com/storagegateway/latest/userguide/StorageGatewayConcepts.html>

**NEW QUESTION 10**

- (Exam Topic 1)

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

```
2 123456789010 eni-1235b8ca123456789 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027 1432917142 ACCEPT OK
2 123456789010 eni-1235b8ca123456789 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094 1432917142 REJECT OK
```

What is one cause of the problem?

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

**Answer: D**

**NEW QUESTION 13**

- (Exam Topic 1)

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.

**Answer: D**

**Explanation:**

It's a best practice to use aws s3 commands (such as aws s3 cp) for multipart uploads and downloads, because these aws s3 commands automatically perform multipart uploading and downloading based on the file size. By comparison, aws s3api commands, such as aws s3api create-multipart-upload, should be used only when aws s3 commands don't support a specific upload need, such as when the multipart upload involves multiple servers, a multipart upload is manually stopped and resumed later, or when the aws s3 command doesn't support a required request parameter.

<https://aws.amazon.com/premiumsupport/knowledge-center/s3-multipart-upload-cli/>

**NEW QUESTION 16**

- (Exam Topic 1)

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

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

**Answer: C**

**Explanation:**

[docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html](https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html)

**NEW QUESTION 21**

- (Exam Topic 1)

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

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

M. Subscribe the SysOps team email address to the SNS topic.

**Answer:** B

**Explanation:**

You can create an Amazon CloudWatch alarm that monitors an Amazon EC2 instance and automatically recovers the instance if it becomes impaired due to an underlying hardware failure or a problem that requires AWS involvement to repair. Terminated instances cannot be recovered. A recovered instance is identical to the original instance, including the instance ID, private IP addresses, Elastic IP addresses, and all instance metadata. If the impaired instance has a public IPv4 address, the instance retains the public IPv4 address after recovery. If the impaired instance is in a placement group, the recovered instance runs in the placement group. When the StatusCheckFailed\_System alarm is triggered, and the recover action is initiated, you will be notified by the Amazon SNS topic that you selected when you created the alarm and associated the recover action. <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-recover.html>

**NEW QUESTION 22**

- (Exam Topic 1)

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 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.

**Answer:** D

**Explanation:**

To make the application accessible only through the CloudFront distribution and not directly through the Application Load Balancer (ALB), you can add a custom HTTP header to the origin settings for the CloudFront distribution. You can then create a rule in the ALB listener to forward requests that contain the matching custom header and its value to the origin. You can also add a default rule to the ALB listener to return a fixed response code of 403 for requests that do not contain the matching custom header. This will allow you to redirect all requests to the CloudFront distribution and block direct access to the application through the ALB. <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/restrict-access-to-load-balancer.html>

**NEW QUESTION 27**

- (Exam Topic 1)

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

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

**Answer:** D

**Explanation:**

Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and troubleshoot issues.

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html>

**NEW QUESTION 29**

- (Exam Topic 1)

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.

**Answer:** B

**NEW QUESTION 32**

- (Exam Topic 1)

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

Which action will allow the SysOps administrator to remotely connect to the instance?

- A. Add a route table entry in the public subnet for the SysOps administrator's IP address.
- B. Add an outbound network ACL rule to allow TCP port 22 for the SysOps administrator's IP address.
- C. Modify the instance security group to allow inbound SSH traffic from the SysOps administrator's IP address.
- D. Modify the instance security group to allow outbound SSH traffic to the SysOps administrator's IP address.

**Answer:** C

#### NEW QUESTION 35

- (Exam Topic 1)

A software company runs a workload on Amazon EC2 instances behind an Application Load Balancer (ALB). A SysOps administrator needs to define a custom health check for the EC2 instances. What is the MOST operationally efficient solution?

- A. Set up each EC2 Instance so that it writes its healthy/unhealthy status into a shared Amazon S3 bucket for the ALB to read
- B. Configure the health check on the ALB and ensure that the HealthCheckPath setting is correct
- C. Set up Amazon ElastiCache to track the EC2 instances as they scale in and out
- D. Configure an Amazon API Gateway health check to ensure custom checks on any of the EC2 instances

**Answer:** B

#### NEW QUESTION 39

- (Exam Topic 1)

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
- B. Deploy the template in each of the accounts
- C. Create an AWS Lambda function to assume a role in each account. Deploy the template by using the AWS CloudFormation CreateStack API call.
- D. Create an AWS Lambda function to query for a list of accounts. Deploy the template by using the AWS CloudFormation CreateStack API call.
- E. Use AWS CloudFormation StackSets from the management account to deploy the template in each of the accounts

**Answer:** D

#### Explanation:

AWS CloudFormation StackSets extends the capability of stacks by enabling you to create, update, or delete stacks across multiple accounts and AWS Regions.

#### NEW QUESTION 40

- (Exam Topic 1)

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
- B. Promote the replica to replace the primary DB instance.
- C. Create an AWS Lambda function to restore an automatic backup to the existing DB cluster.
- D. Use backtracking to rewind the existing DB cluster to the desired recovery point.
- E. Use point-in-time recovery to restore the existing DB cluster to the desired recovery point.

**Answer:** C

#### Explanation:

"The limit for a backtrack window is 72 hours....Backtracking is only available for DB clusters that were created with the Backtrack feature enabled....Backtracking "rewinds" the DB cluster to the time you specify. Backtracking is not a replacement for backing up your DB cluster so that you can restore it to a point in time....You can backtrack a DB cluster quickly. Restoring a DB cluster to a point in time launches a new DB cluster and restores it from backup data or a DB cluster snapshot, which can take hours."

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Managing.Backtrack.html>

#### NEW QUESTION 43

- (Exam Topic 1)

A SysOps administrator is testing an application that is hosted on five Amazon EC2 instances. The instances run in an Auto Scaling group behind an Application Load Balancer (ALB). High CPU utilization during load testing is causing the Auto Scaling group to scale out. The SysOps administrator must troubleshoot to find the root cause of the high CPU utilization before the Auto Scaling group scales out.

Which action should the SysOps administrator take to meet these requirements?

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

**Answer:** A

#### NEW QUESTION 47

- (Exam Topic 1)

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 12 large instances to the application
- D. Purchase Reserved Instances

**Answer:** B

#### NEW QUESTION 48

- (Exam Topic 1)

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.

**Answer:** CE

#### Explanation:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/default-bucket-encryption.html>

You can set the default encryption behavior on an Amazon S3 bucket so that all objects are encrypted when they are stored in the bucket. The objects are encrypted using server-side encryption with either Amazon S3-managed keys (SSE-S3) or AWS Key Management Service (AWS KMS) customer master keys (CMKs).

<https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/> How to Prevent Uploads of Unencrypted Objects to Amazon S3#

By using an S3 bucket policy, you can enforce the encryption requirement when users upload objects, instead of assigning a restrictive IAM policy to all users.

#### NEW QUESTION 52

- (Exam Topic 1)

A company recently acquired another corporation and all of that corporation's AWS accounts. A financial analyst needs the cost data from these accounts. A SysOps administrator uses Cost Explorer to generate cost and usage reports. The SysOps administrator notices that "No Tagkey" represents 20% of the monthly cost.

What should the SysOps administrator do to tag the "No Tagkey" resources?

- A. Add the accounts to AWS Organization
- B. Use a service control policy (SCP) to tag all the untagged resources.
- C. Use an AWS Config rule to find the untagged resource
- D. Set the remediation action to terminate the resources.
- E. Use Cost Explorer to find and tag all the untagged resources.
- F. Use Tag Editor to find and tag all the untagged resources.

**Answer:** D

#### Explanation:

"You can add tags to resources when you create the resource. You can use the resource's service console or API to add, change, or remove those tags one resource at a time. To add tags to—or edit or delete tags of—multiple resources at once, use Tag Editor. With Tag Editor, you search for the resources that you want to tag, and then manage tags for the resources in your search results." <https://docs.aws.amazon.com/ARG/latest/userguide/tag-editor.html>

#### NEW QUESTION 55

- (Exam Topic 1)

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
- B. Configure the Lambda function to compute an MD5 hash check on the file and store the result in an Amazon DynamoDB table
- C. The security team can use the values that are stored in DynamoDB to verify the integrity of the delivered files.
- D. Create an AWS Lambda function that is invoked each time a new file is delivered to the CloudTrail bucket
- E. Configure the Lambda function to compute an MD5 hash check on the file and store the result as a tag in an Amazon S3 object
- F. The security team can use the information in the tag to verify the integrity of the delivered files.
- G. Enable the CloudTrail file integrity feature on an Amazon S3 bucket
- H. Create an IAM policy that grants the security team access to the file integrity logs that are stored in the S3 bucket.
- I. Enable the CloudTrail file integrity feature on the trail
- J. The security team can use the digest file that is created by CloudTrail to verify the integrity of the delivered files.

**Answer:** D

#### Explanation:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html> "When you enable log file integrity validation, CloudTrail creates a hash for every log file that it delivers.

Every hour, CloudTrail also creates and delivers a file that references the log files for the last hour and contains a hash of each. This file is called a digest file. Validated log files are invaluable in security and forensic investigations"

#### NEW QUESTION 56

- (Exam Topic 1)

A company has deployed a web application in a VPC that has subnets in three Availability Zones. The company launches three Amazon EC2 instances from an EC2 Auto Scaling group behind an Application Load Balancer (ALB).

A SysOps administrator notices that two of the EC2 instances are in the same Availability Zone, rather than being distributed evenly across all three Availability Zones. There are no errors in the Auto Scaling group's activity history. What is the MOST likely reason for the unexpected placement of EC2 instances?

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

**Answer:** C

**Explanation:**

the autoscaling group is responsible to add the instances in the subnets

**NEW QUESTION 57**

- (Exam Topic 1)

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

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

**Answer:** D

**Explanation:**

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

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/redis-cluster-vertical-scaling-scaling-down.html>

**NEW QUESTION 59**

- (Exam Topic 1)

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

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

**Answer:** A

**NEW QUESTION 61**

- (Exam Topic 1)

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

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

**Answer:** C

**NEW QUESTION 65**

- (Exam Topic 1)

A company stores critical data in Amazon S3 buckets. A SysOps administrator must build a solution to record all S3 API activity. Which action will meet this requirement?

- A. Configure S3 bucket metrics to record object access logs.
- B. Create an AWS CloudTrail trail to log data events for all S3 objects.
- C. Enable S3 server access logging for each S3 bucket.
- D. Use AWS IAM Access Analyzer for Amazon S3 to store object access logs.

**Answer:** B

**NEW QUESTION 69**

- (Exam Topic 1)

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

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

**Answer: C**

#### NEW QUESTION 72

- (Exam Topic 1)

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

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

**Answer: B**

#### NEW QUESTION 76

- (Exam Topic 1)

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

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

**Answer: A**

#### NEW QUESTION 78

- (Exam Topic 1)

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 81

- (Exam Topic 1)

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

**Answer: B**

**NEW QUESTION 84**

- (Exam Topic 1)

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

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

**Answer: A**

**NEW QUESTION 88**

- (Exam Topic 1)

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.

**Answer: AC**

**NEW QUESTION 90**

- (Exam Topic 1)

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 instances, 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.

**Answer: B**

**NEW QUESTION 95**

- (Exam Topic 1)

A company is using Amazon Elastic Container Service (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.

**Answer: AE**

**NEW QUESTION 98**

- (Exam Topic 1)

A company is using Amazon CloudFront to serve static content for its web application to its users. The CloudFront distribution uses an existing on-premises website as a custom origin.

The company requires the use of TLS between CloudFront and the origin server. This configuration has worked as expected for several months. However, users are now experiencing HTTP 502 (Bad Gateway) errors when they view webpages that include content from the CloudFront distribution. What should a SysOps administrator do to resolve this problem?

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

**Answer:** A

**Explanation:**

HTTP 502 errors from CloudFront can occur because of the following reasons:

There's an SSL negotiation failure because the origin is using SSL/TLS protocols and ciphers that aren't supported by CloudFront.

There's an SSL negotiation failure because the SSL certificate on the origin is expired or invalid, or because the certificate chain is invalid.

There's a host header mismatch in the SSL negotiation between your CloudFront distribution and the custom origin.

The custom origin isn't responding on the ports specified in the origin settings of the CloudFront distribution. The custom origin is ending the connection to CloudFront too quickly.

<https://aws.amazon.com/premiumsupport/knowledge-center/resolve-cloudfront-connection-error/>

**NEW QUESTION 100**

- (Exam Topic 1)

Application A runs on Amazon EC2 instances behind a Network Load Balancer (NLB). The EC2 instances are in an Auto Scaling group and are in the same subnet that is associated with the NLB. Other applications from an on-premises environment cannot communicate with Application A on port 8080. To troubleshoot the issue, a SysOps administrator analyzes the flow logs. The flow logs include the following records:

```
2 123456789010 eni-1235b8ca123456789 192.168.0.13 172.31.16.139 59003 8080 1 4 336 1432917027 1432917142 ACCEPT OK
2 123456789010 eni-1235b8ca123456789 172.31.16.139 192.168.0.13 8080 59003 1 4 336 1432917094 1432917142 REJECT OK
```

What is the reason for the rejected traffic?

- A. The security group of the EC2 instances has no Allow rule for the traffic from the NLB.
- B. The security group of the NLB has no Allow rule for the traffic from the on-premises environment.
- C. The ACL of the on-premises environment does not allow traffic to the AWS environment.
- D. The network ACL that is associated with the subnet does not allow outbound traffic for the ephemeral port range.

**Answer:** A

**NEW QUESTION 105**

- (Exam Topic 1)

A company runs its entire suite of applications on Amazon EC2 instances. The company plans to move the applications to containers and AWS Fargate. Within 6 months, the company plans to retire its EC2 instances and use only Fargate. The company has been able to estimate its future Fargate costs.

A SysOps administrator needs to choose a purchasing option to help the company minimize costs. The SysOps administrator must maximize any discounts that are available and must ensure that there are no unused reservations.

Which purchasing option will meet these requirements?

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

**Answer:** C

**NEW QUESTION 109**

- (Exam Topic 1)

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 each 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.

**Answer:** C

**NEW QUESTION 111**

- (Exam Topic 1)

A SysOps administrator has Nocked public access to all company Amazon S3 buckets. The SysOps administrator wants to be notified when an S3 bucket becomes publicly readable in the future.

What is the MOST operationally efficient way to meet this requirement?

- A. Create an AWS Lambda function that periodically checks the public access settings for each S3 bucket. Set up Amazon Simple Notification Service (Amazon SNS) to send notifications.
- B. Create a cron script that uses the S3 API to check the public access settings for each S3 bucket.
- C. Set up Amazon Simple Notification Service (Amazon SNS) to send notifications
- D. Enable S3 Event notifications for each S3 bucket
- E. Subscribe S3 Event Notifications to an Amazon Simple Notification Service (Amazon SNS) topic.
- F. Enable the s3-bucket-public-read-prohibited managed rule in AWS Config
- G. Subscribe the AWS Config rule to an Amazon Simple Notification Service (Amazon SNS) topic.

**Answer: D**

#### NEW QUESTION 114

- (Exam Topic 1)

A Sysops administrator needs to configure automatic rotation for Amazon RDS database credentials. The credentials must rotate every 30 days. The solution must integrate with Amazon RDS.

Which solution will meet these requirements with the LEAST operational overhead?

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 116

- (Exam Topic 1)

A SysOps administrator needs to track the costs of data transfer between AWS Regions. The SysOps administrator must implement a solution to send alerts to an email distribution list when transfer costs reach 75% of a specific threshold.

What should the SysOps administrator do to meet these requirements?

- A. Create an AWS Cost and Usage Report
- B. Analyze the results in Amazon Athena
- C. Configure an alarm to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic when costs reach 75% of the threshold
- D. Subscribe the email distribution list to the topic.
- E. Create an Amazon CloudWatch billing alarm to detect when costs reach 75% of the threshold. Configure the alarm to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic
- F. Subscribe the email distribution list to the topic.
- G. Use AWS Budgets to create a cost budget for data transfer cost
- H. Set an alert at 75% of the budgeted amount
- I. Configure the budget to send a notification to the email distribution list when costs reach 75% of the threshold.
- J. Set up a VPC flow log
- K. Set up a subscription filter to an AWS Lambda function to analyze data transfer. Configure the Lambda function to send a notification to the email distribution list when costs reach 75% of the threshold.

**Answer: B**

#### Explanation:

The reason is that it uses the Amazon CloudWatch billing alarm which is a built-in service specifically designed to monitor and alert on cost usage of your AWS account, which makes it a more suitable solution for this use case. The alarm can be configured to detect when costs reach 75% of the threshold and when it is triggered, it can publish a message to an Amazon Simple Notification Service (Amazon SNS) topic. The email distribution list can be subscribed to the topic, so that they will receive the alerts when costs reach 75% of the threshold.

AWS Budgets allows you to track and manage your costs, but it doesn't specifically focus on data transfer costs between regions, and it might not provide as much granularity as CloudWatch Alarms.

#### NEW QUESTION 119

- (Exam Topic 1)

A Sysops administrator creates an Amazon Elastic Kubernetes Service (Amazon EKS) cluster that uses AWS Fargate. The cluster is deployed successfully. The Sysops administrator needs to manage the cluster by using the kubectl command line tool.

Which of the following must be configured on the Sysops administrator's machine so that kubectl can communicate with the cluster API server?

- A. The kubeconfig file
- B. The kube-proxy Amazon EKS add-on
- C. The Fargate profile
- D. The eks-connector.yaml file

**Answer: A**

**Explanation:**

The kubeconfig file is a configuration file used to store cluster authentication information, which is required to make requests to the Amazon EKS cluster API server. The kubeconfig file will need to be configured on the SysOps administrator's machine in order for kubectl to be able to communicate with the cluster API server.

<https://aws.amazon.com/blogs/developer/running-a-kubernetes-job-in-amazon-eks-on-aws-fargate-using-aws-ste>

**NEW QUESTION 124**

- (Exam Topic 1)

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 metri
- B. Configure an action to send an Amazon Simple Notification Service (Amazon SNS) notification when the metric is greater than 0.
- C. 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.
- D. Update the Auto Scaling grou
- E. Configure an activity notification to send an Amazon Simple Notification Service (Amazon SNS) notification for the Unhealthy event type.
- F. Update the ALB health check to send an Amazon Simple Notification Service (Amazon SNS) notification when an instance is unhealthy.

**Answer:** A

**NEW QUESTION 127**

- (Exam Topic 1)

A company needs to automatically monitor an AWS account for potential unauthorized AWS Management Console logins from multiple geographic locations. Which solution will meet this requirement?

- A. Configure Amazon Cognito to detect any compromised IAM credentials.
- B. Set up Amazon Inspector
- C. Scan and monitor resources for unauthorized logins.
- D. Set up AWS Confi
- E. Add the iam-policy-blacklisted-check managed rule to the account.
- F. Configure Amazon GuardDuty to monitor the UnauthorizedAccess:IAMUser/ConsoleLoginSuccess finding.

**Answer:** D

**NEW QUESTION 132**

- (Exam Topic 1)

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

**Answer:** A

**Explanation:**

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ri-convertible-exchange.html>

**NEW QUESTION 135**

- (Exam Topic 1)

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

**Answer:** D

**Explanation:**

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingEncryption.html>

**NEW QUESTION 139**

- (Exam Topic 1)

A SysOps administrator has an AWS CloudFormation template of the company's existing infrastructure in us-west-2. The administrator attempts to use the template to launch a new stack in eu-west-1, but the stack only partially deploys, receives an error message, and then rolls back.

Why would this template fail to deploy? (Select TWO.)

- A. The template referenced an IAM user that is not available in eu-west-1.

- B. The template referenced an Amazon Machine Image (AMI) that is not available in eu-west-1.
- C. The template did not have the proper level of permissions to deploy the resources.
- D. The template requested services that do not exist in eu-west-1.
- E. CloudFormation templates can be used only to update existing services.

**Answer:** BD

#### NEW QUESTION 144

- (Exam Topic 1)

A company needs to ensure strict adherence to a budget for 25 applications deployed on AWS. Separate teams are responsible for storage, compute, and database costs. A SysOps administrator must implement an automated solution to alert each team when their projected spend will exceed a quarterly amount that has been set by the finance department. The solution cannot add additional compute, storage, or database costs.

- A. Configure AWS Cost and Usage Reports to send a daily report to an Amazon S3 bucket.
- B. Create an AWS Lambda function that will evaluate spend by service and notify each team by using Amazon Simple Notification Service (Amazon SNS) notification.
- C. Invoke the Lambda function when a report is placed in the S3 bucket.
- D. Configure AWS Cost and Usage Reports to send a daily report to an Amazon S3 bucket.
- E. Create a rule in Amazon EventBridge (Amazon CloudWatch Events) to evaluate the spend by service and notify each team by using Amazon Simple Queue Service (Amazon SQS) when the cost threshold is exceeded.
- F. Use AWS Budgets to create one cost budget and select each of the services in use. Specify the budget amount defined by the finance department along with the forecasted cost threshold. Enter the appropriate email recipients for the budget.
- G. Use AWS Budgets to create a cost budget for each team, filtering by the services they own.
- H. Specify the budget amount defined by the finance department along with a forecasted cost threshold. Enter the appropriate email recipients for each budget.

**Answer:** D

#### NEW QUESTION 146

- (Exam Topic 1)

A company is expanding its use of AWS services across its portfolios. The company wants to provision AWS accounts for each team to ensure a separation of business processes for security compliance and billing. Account creation and bootstrapping should be completed in a scalable and efficient way so new accounts are created with a defined baseline and governance guardrails in place. A SysOps administrator needs to design a provisioning process that saves time and resources.

Which action should be taken to meet these requirements?

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

**Answer:** D

#### NEW QUESTION 148

- (Exam Topic 1)

A compliance team requires 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.

**Answer:** A

#### NEW QUESTION 149

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 152

- (Exam Topic 1)

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.

**Answer:** B

**Explanation:**

When you enable log file integrity validation, CloudTrail creates a hash for every log file that it delivers. Every hour, CloudTrail also creates and delivers a file that references the log files for the last hour and contains a hash of each. This file is called a digest file. CloudTrail signs each digest file using the private key of a public and private key pair. After delivery, you can use the public key to validate the digest file. CloudTrail uses different key pairs for each AWS region  
<https://docs.aws.amazon.com/awsccloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html>

**NEW QUESTION 155**

- (Exam Topic 1)

A SysOps administrator creates two VPCs, VPC1 and VPC2, in a company's AWS account. The SysOps administrator deploys a Linux Amazon EC2 instance in VPC1 and deploys an Amazon RDS for MySQL DB instance in VPC2. The DB instance is deployed in a private subnet. An application that runs on the EC2 instance needs to connect to the database.

What should the SysOps administrator do to give the EC2 instance the ability to connect to the database?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 156**

- (Exam Topic 1)

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.

**Answer:** AD

**Explanation:**

<https://aws.amazon.com/blogs/security/how-to-receive-alerts-when-your-iam-configuration-changes/>

**NEW QUESTION 159**

- (Exam Topic 1)

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.

**Answer:** B

**Explanation:**

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scps.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html)

If you're using AWS Organizations, check the service control policies for any statements that explicitly deny Amazon S3 access. In particular, check the service control policies for statements denying the s3:PutBucketPolicy action.

<https://aws.amazon.com/tw/premiumsupport/knowledge-center/s3-access-denied-bucket-policy/>

**NEW QUESTION 161**

- (Exam Topic 1)

An AWS Lambda function is intermittently failing several times a day. A SysOps administrator must find out how often this error has occurred in the last 7 days.

Which action will meet this requirement in the MOST operationally efficient manner?

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

**Answer:** C

**NEW QUESTION 166**

- (Exam Topic 1)

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.

**Answer: D**

#### NEW QUESTION 169

- (Exam Topic 1)

A manufacturing company uses an Amazon RDS DB instance to store inventory of all stock items. The company maintains several AWS Lambda functions that interact with the database to add, update, and delete items. The Lambda functions use hardcoded credentials to connect to the database.

A SysOps administrator must ensure that the database credentials are never stored in plaintext and that the password is rotated every 30 days.

Which solution will meet these requirements in the MOST operationally efficient manner?

- A. Store the database password as an environment variable for each Lambda function.
- B. Create a new Lambda function that is named PasswordRotate.
- C. Use Amazon EventBridge (Amazon CloudWatch Events) to schedule the PasswordRotate function every 30 days to change the database password and update the environment variable for each Lambda function.
- D. Use AWS Key Management Service (AWS KMS) to encrypt the database password and to store the encrypted password as an environment variable for each Lambda function.
- E. Grant each Lambda function access to the KMS key so that the database password can be decrypted when required.
- F. Create a new Lambda function that is named PasswordRotate to change the password every 30 days.
- G. Use AWS Secrets Manager to store credentials for the databases.
- H. Create a Secrets Manager secret, and select the database so that Secrets Manager will use a Lambda function to update the database password automatically.
- I. Specify an automatic rotation schedule of 30 days.
- J. Update each Lambda function to access the database password from Secrets Manager.
- K. Use AWS Systems Manager Parameter Store to create a secure string to store credentials for the databases.
- L. Create a new Lambda function called PasswordRotate.
- M. Use Amazon EventBridge (Amazon CloudWatch Events) to schedule the PasswordRotate function every 30 days to change the database password and to update the secret within Parameter Store.
- N. Update each Lambda function to access the database password from Parameter Store.

**Answer: C**

#### Explanation:

When you choose to enable rotation, Secrets Manager supports the following Amazon Relational Database Service (Amazon RDS) databases with AWS written and tested Lambda rotation function templates, and full configuration of the rotation process:

Amazon Aurora on Amazon RDS MySQL on Amazon RDS PostgreSQL on Amazon RDS Oracle on Amazon RDS MariaDB on Amazon RDS Microsoft SQL Server on Amazon RDS <https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html>

#### NEW QUESTION 171

- (Exam Topic 1)

A company needs to view a list of security groups that are open to the internet on port 3389. What should a SysOps administrator do to meet this requirement?

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

**Answer: D**

#### NEW QUESTION 173

- (Exam Topic 1)

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.

**Answer: A**

#### NEW QUESTION 177

- (Exam Topic 1)

A SysOps administrator is optimizing the cost of a workload. The workload is running in multiple AWS Regions and is using AWS Lambda with Amazon EC2 On-Demand Instances for the compute. The overall usage is predictable. The amount of compute that is consumed in each Region varies, depending on the users' locations.

Which approach should the SysOps administrator use to optimize this workload?

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

**Answer: C**

#### NEW QUESTION 179

- (Exam Topic 1)

A company is expanding its fleet of Amazon EC2 instances before an expected increase of traffic. When a SysOps administrator attempts to add more instances, an InstanceLimitExceeded error is returned.

What should the SysOps administrator do to resolve this error?

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

**Answer: D**

#### NEW QUESTION 182

- (Exam Topic 1)

A company runs an application on an Amazon EC2 instance. A SysOps administrator creates an Auto Scaling group and an Application Load Balancer (ALB) to handle an increase in demand. However, the EC2 instances are failing the health check.

What should the SysOps administrator do to troubleshoot this issue?

- A. Verify that the Auto Scaling group is configured to use all AWS Regions.
- B. Verify that the application is running on the protocol and the port that the listener is expecting.
- C. Verify the listener priority in the ALB. Change the priority if necessary.
- D. Verify the maximum number of instances in the Auto Scaling group. Change the number if necessary.

**Answer: B**

#### NEW QUESTION 183

- (Exam Topic 1)

A company hosts a web portal on Amazon EC2 instances. The web portal uses an Elastic Load Balancer (ELB) and Amazon Route 53 for its public DNS service. The ELB and the EC2 instances are deployed by way of a single AWS CloudFormation stack in the us-east-1 Region. The web portal must be highly available across multiple Regions.

Which configuration will meet these requirements?

- A. Deploy a copy of the stack in the us-west-2 Region
- B. Create a single start of authority (SOA) record in Route 53 that includes the IP address from each ELB
- C. Configure the SOA record with health check
- D. Use the ELB in us-east-1 as the primary record and the ELB in us-west-2 as the secondary record.
- E. Deploy a copy of the stack in the us-west-2 Region
- F. Create an additional A record in Route 53 that includes the ELB in us-west-2 as an alias target
- G. Configure the A records with a failover routing policy and health check
- H. Use the ELB in us-east-1 as the primary record and the ELB in us-west-2 as the secondary record.
- I. Deploy a new group of EC2 instances in the us-west-2 Region
- J. Associate the new EC2 instances with the existing ELB, and configure load balancer health checks on all EC2 instances
- K. Configure the ELB to update Route 53 when EC2 instances in us-west-2 fail health checks.
- L. Deploy a new group of EC2 instances in the us-west-2 Region
- M. Configure EC2 health checks on all EC2 instances in each Region
- N. Configure a peering connection between the VPC
- O. Use the VPC in us-east-1 as the primary record and the VPC in us-west-2 as the secondary record.

**Answer: B**

#### Explanation:

When you create a hosted zone, Route 53 automatically creates a name server (NS) record and a start of authority (SOA) record for the zone.

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/migrate-dns-domain-in-use.html#migrate-dns-crea>

[https://en.wikipedia.org/wiki/SOA\\_record](https://en.wikipedia.org/wiki/SOA_record)

#### NEW QUESTION 187

- (Exam Topic 1)

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 IAM 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.

**Answer: B**

**NEW QUESTION 188**

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

**Answer: C**

**NEW QUESTION 191**

- (Exam Topic 1)

A company needs to take an inventory of applications that are running on multiple Amazon EC2 instances. The company has configured users and roles with the appropriate permissions for AWS Systems Manager. An updated version of Systems Manager Agent has been installed and is running on every instance. While configuring an inventory collection, a SysOps administrator discovers that not all the instances in a single subnet are managed by Systems Manager.

What must the SysOps administrator do to fix this issue?

- A. Ensure that all the EC2 instances have the correct tags for Systems Manager access.
- B. Configure AWS Identity and Access Management Access Analyzer to determine and automatically remediate the issue.
- C. Ensure that all the EC2 instances have an instance profile with Systems Manager access.
- D. Configure Systems Manager to use an interface VPC endpoint.

**Answer: C**

**Explanation:**

Ensuring that all the EC2 instances have an instance profile with Systems Manager access is the most effective way to fix this issue. Having an instance profile with Systems Manager access will allow the SysOps administrator to configure the inventory collection for all the instances in the subnet, regardless of whether or not they are managed by Systems Manager.

**NEW QUESTION 195**

- (Exam Topic 1)

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

**Answer: B**

**NEW QUESTION 200**

- (Exam Topic 1)

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

How can this be accomplished?

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

**Answer: B**

**NEW QUESTION 204**

- (Exam Topic 1)

A SysOps administrator is tasked with deploying a company's infrastructure as code. The SysOps administrator wants to write a single template that can be reused for multiple environments.

How should the SysOps administrator use AWS CloudFormation to create a solution?

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

**Answer: C**

**Explanation:**

Reuse templates to replicate stacks in multiple environments. After you have your stacks and resources set up, you can reuse your templates to replicate your

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

**NEW QUESTION 207**

- (Exam Topic 1)

A SysOps administrator developed a Python script that uses the AWS SDK to conduct several maintenance tasks. The script needs to run automatically every night.

What is the MOST operationally efficient solution that meets this requirement?

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

**Answer:** A

**NEW QUESTION 212**

- (Exam Topic 1)

A company has a memory-intensive application that runs on a fleet of Amazon EC2 instances behind an Elastic Load Balancer (ELB). The instances run in an Auto Scaling group. A Sysops administrator must ensure that the application can scale based on the number of users that connect to the application.

Which solution will meet these requirements?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 214**

- (Exam Topic 1)

A company's SysOps administrator must ensure that all Amazon EC2 Windows instances that are launched in an AWS account have a third-party agent installed. The third-party agent has an msi package. The company uses AWS Systems Manager for patching, and the Windows instances are tagged appropriately. The third-party agent required periodic updates as new versions are released. The SysOps administrator must deploy these updates automatically. Which combination of steps will meet these requirements with the LEAST operational effort? (Seed TWO.) Create a Systems Manager Distributor package for the third-party agent.

- A. Make sure that Systems Manager Inventory Is configure
- B. If Systems Manager Inventory is not configured, set up a new inventory tor instances that is based on the appropriate tag value for Windows.
- C. Create a Systems Manager State Manager association to run the AWS-RunRemoteScript document.Populate the details of the third-party agent packag
- D. Specify instance tags based on the appropriate tag value for Windows with a schedule of 1 day
- E. Create a Systems Manager State Manager- association to run the AWS-ConfigureAWSPackage documen
- F. Populate the details of the third-party agent packag
- G. Specify instance tags based on the appropriate tag value for Windows with a schedule of 1 day
- H. Create a Systems Manager Opsitem with the tag value for Windows Attach the Systems Manager Distributor package to the Opsite
- I. Create a maintenance window that is specific to the package deployment Configure the maintenance window to cover 24 hours a day.

**Answer:** AD

**Explanation:**

<https://docs.aws.amazon.com/systems-manager/latest/userguide/distributor-working-with-packages-deploy.html>

**NEW QUESTION 217**

- (Exam Topic 1)

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 single AWS Region

**Answer:** D

**Explanation:**

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

**NEW QUESTION 219**

- (Exam Topic 1)

A compliance learn requires 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
- B. Configure automatic rotation for the secret every 365 days.
- C. Store the database credentials as a parameter in the RDS parameter group
- D. Create a database trigger to rotate the password every 365 days.
- E. Store the database credentials in a private Amazon S3 bucket
- F. Schedule an AWS Lambda function to generate a new set of credentials every 365 days.
- G. Store the database credentials in AWS Systems Manager Parameter Store as a secure string parameter. Configure automatic rotation for the parameter every 365 days.

**Answer: A**

**NEW QUESTION 221**

- (Exam Topic 1)

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.

**Answer: B**

**NEW QUESTION 223**

- (Exam Topic 1)

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.

**Answer: B**

**NEW QUESTION 226**

- (Exam Topic 2)

A webpage is stored in an Amazon S3 bucket behind an Application Load Balancer (ALB). Configure the S3 bucket to serve a static error page in the event of a failure at the primary site.

- \* 1. Use the us-east-2 Region for all resources.
- \* 2. Unless specified below, use the default configuration settings.
- \* 3. There is an existing hosted zone named lab-751906329398-26023898.com that contains an A record with a simple routing policy that routes traffic to an existing ALB.
- \* 4. Configure the existing S3 bucket named lab-751906329398-26023898.com as a static hosted website using the object named index.html as the index document
- \* 5. For the index.html object, configure the S3 ACL to allow for public read access. Ensure public access to the S3 bucket is allowed.
- \* 6. In Amazon Route 53, change the A record for domain lab-751906329398-26023898.com to a primary record for a failover routing policy. Configure the record so that it evaluates the health of the ALB to determine failover.
- \* 7. Create a new secondary failover alias record for the domain lab-751906329398-26023898.com that routes traffic to the existing S3 bucket.

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Here are the steps to configure an Amazon S3 bucket to serve a static error page in the event of a failure at the primary site:

- Log in to the AWS Management Console and navigate to the S3 service in the us-east-2 Region.
- Find the existing S3 bucket named lab-751906329398-26023898.com and click on it.
- In the "Properties" tab, click on "Static website hosting" and select "Use this bucket to host a website".
- In "Index Document" field, enter the name of the object that you want to use as the index document, in this case, "index.html"
- In the "Permissions" tab, click on "Block Public Access", and make sure that "Block all public access" is turned OFF.
- Click on "Bucket Policy" and add the following policy to allow public read access:

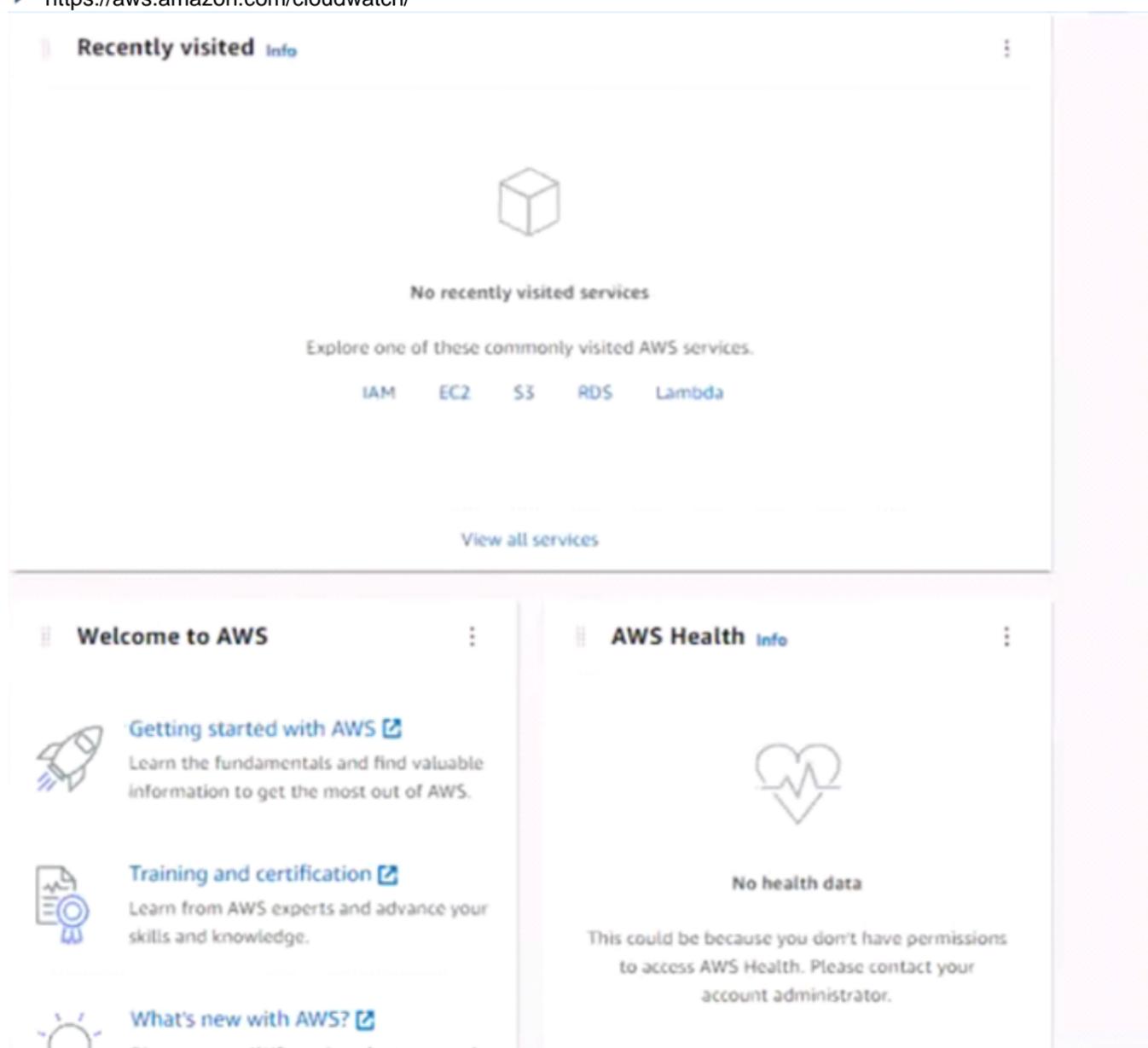
```
{  
  "Version": "2012-10-17",
```

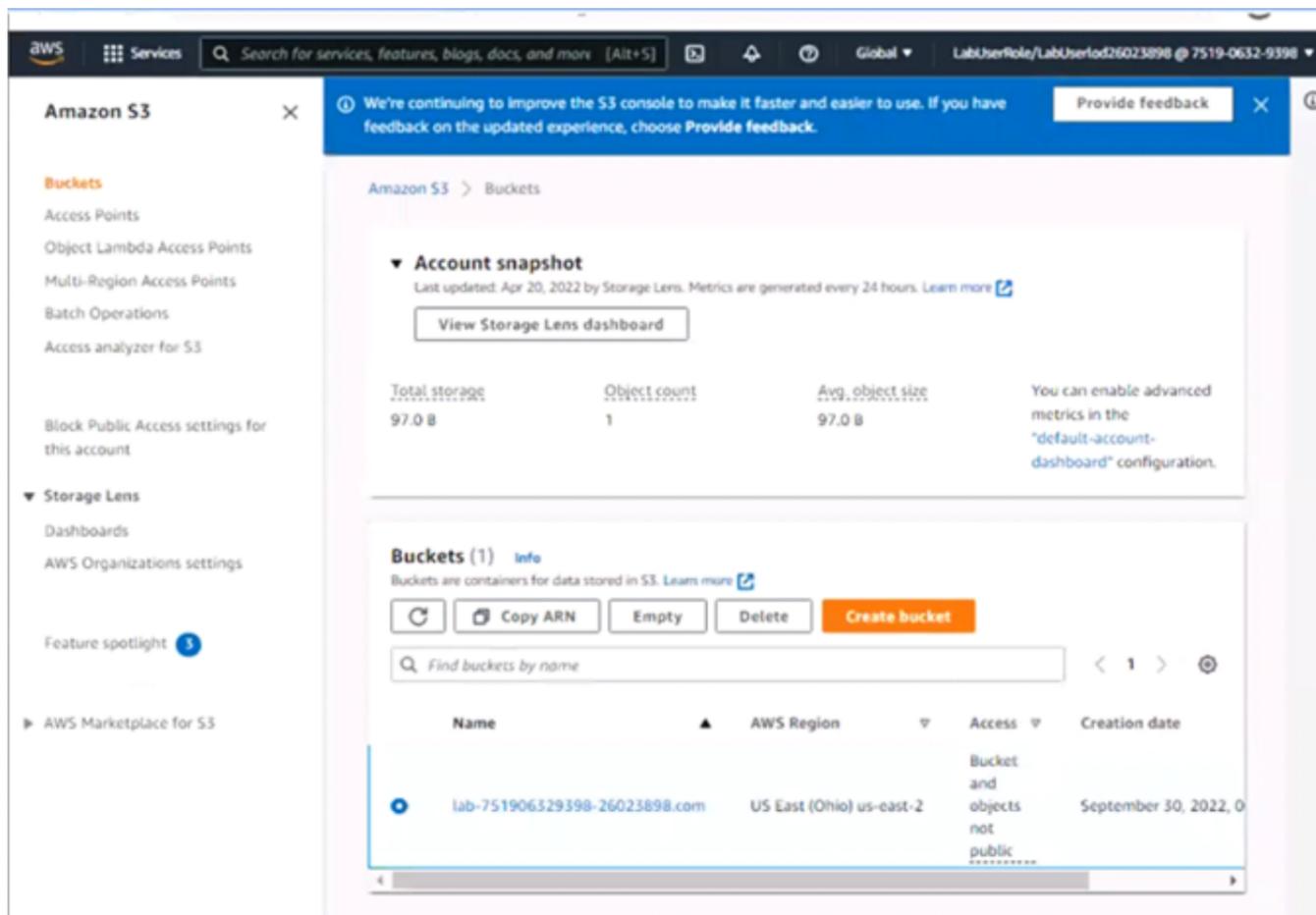
```
"Statement": [
{
  "Sid": "PublicReadGetObject", "Effect": "Allow",
  "Principal": "*", "Action": "s3:GetObject",
  "Resource": "arn:aws:s3:::lab-751906329398-26023898.com/*"
}
]
```

- Now navigate to the Amazon Route 53 service, and find the existing hosted zone named lab-751906329398-26023898.com.
- Click on the "A record" and update the routing policy to "Primary - Failover" and add the existing ALB as the primary record.
- Click on "Create Record" button and create a new secondary failover alias record for the domain lab-751906329398-26023898.com that routes traffic to the existing S3 bucket.
- Now, when the primary site (ALB) goes down, traffic will be automatically routed to the S3 bucket serving the static error page.

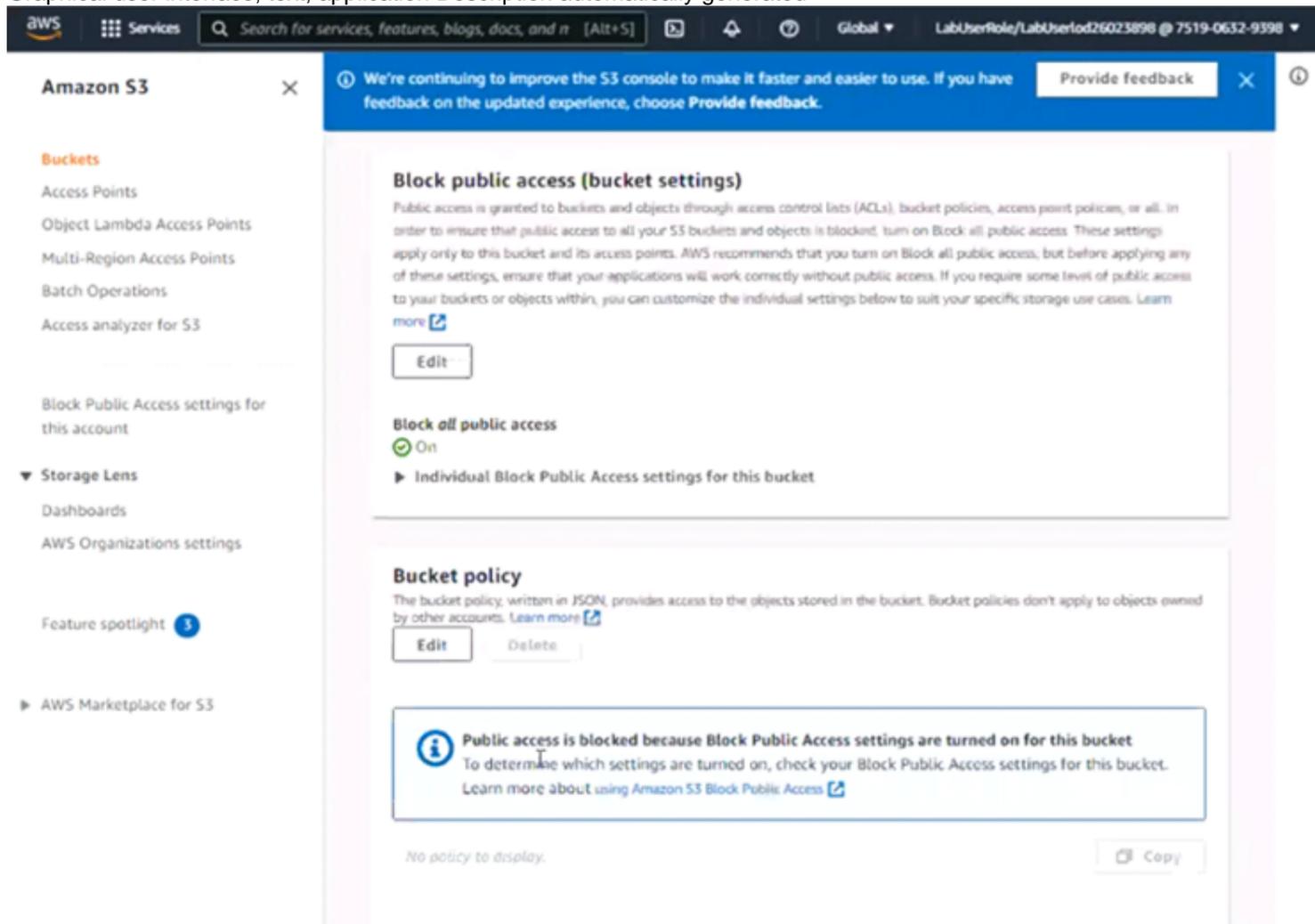
Note:

- You can use CloudWatch to monitor the health of your ALB.
- You can use Amazon S3 to host a static website.
- You can use Amazon Route 53 for routing traffic to different resources based on health checks.
- You can refer to the AWS documentation for more information on how to configure and use these services:
- <https://aws.amazon.com/s3/>
- <https://aws.amazon.com/route53/>
- <https://aws.amazon.com/cloudwatch/>

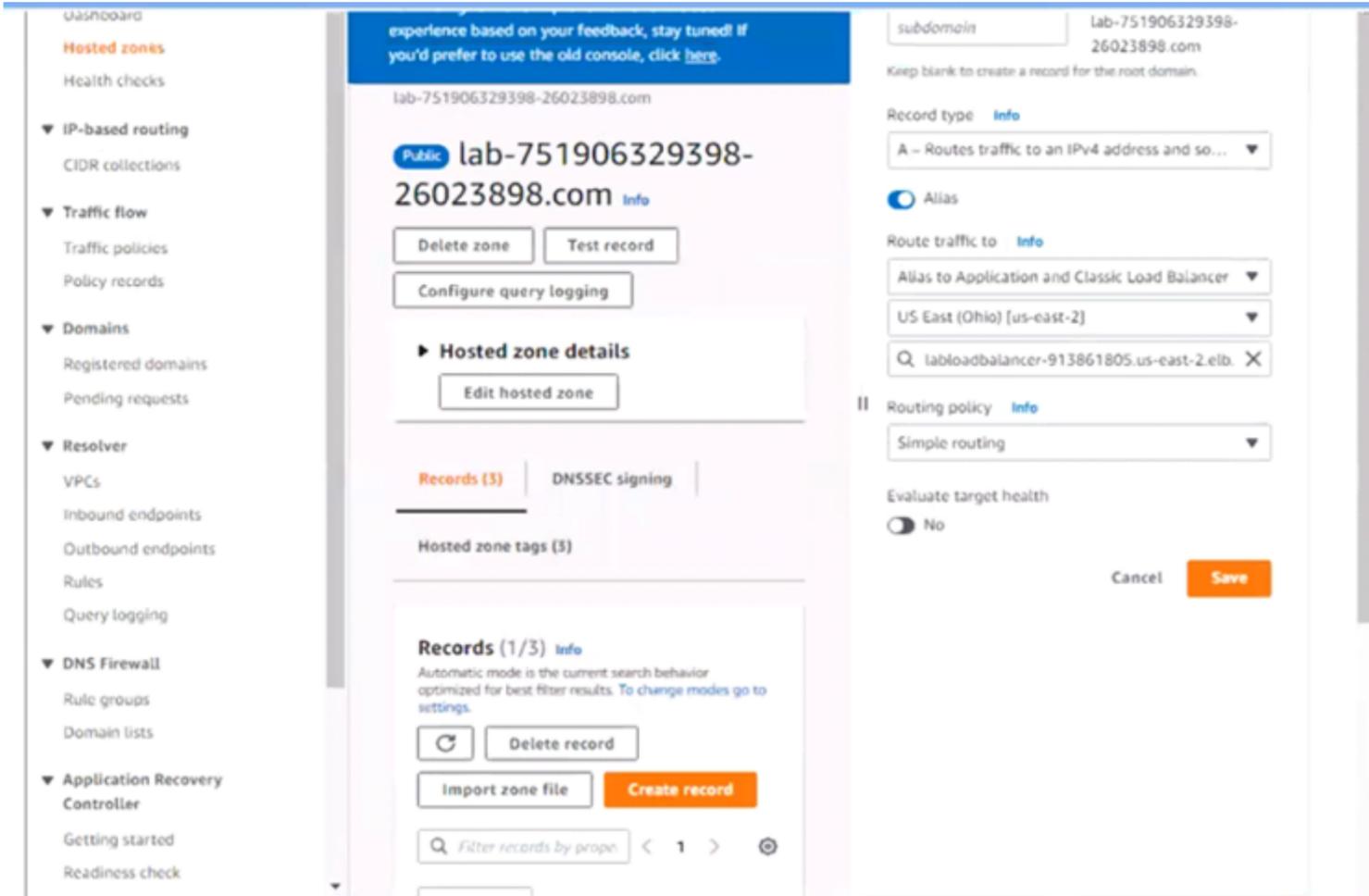




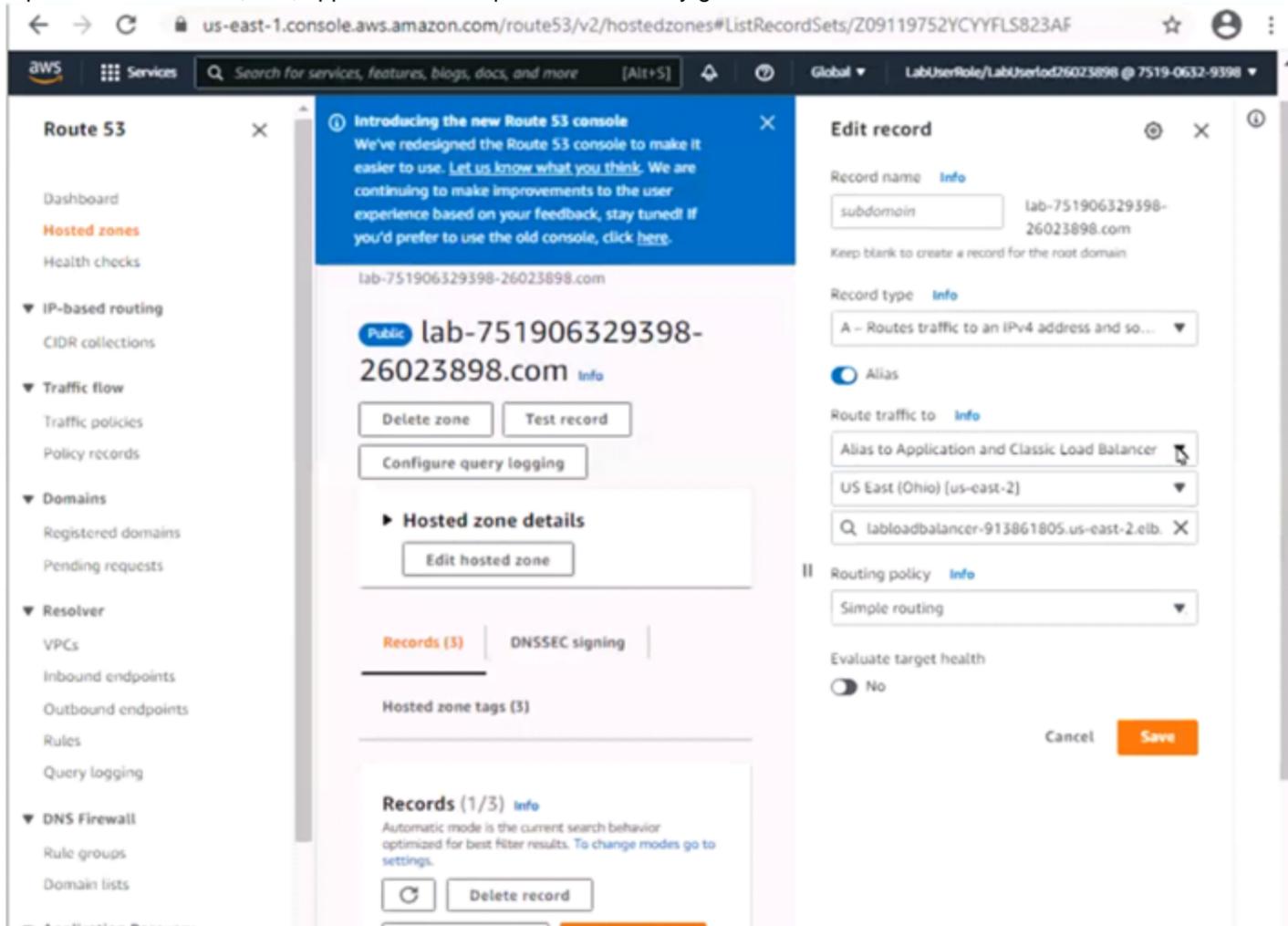
Graphical user interface, text, application Description automatically generated

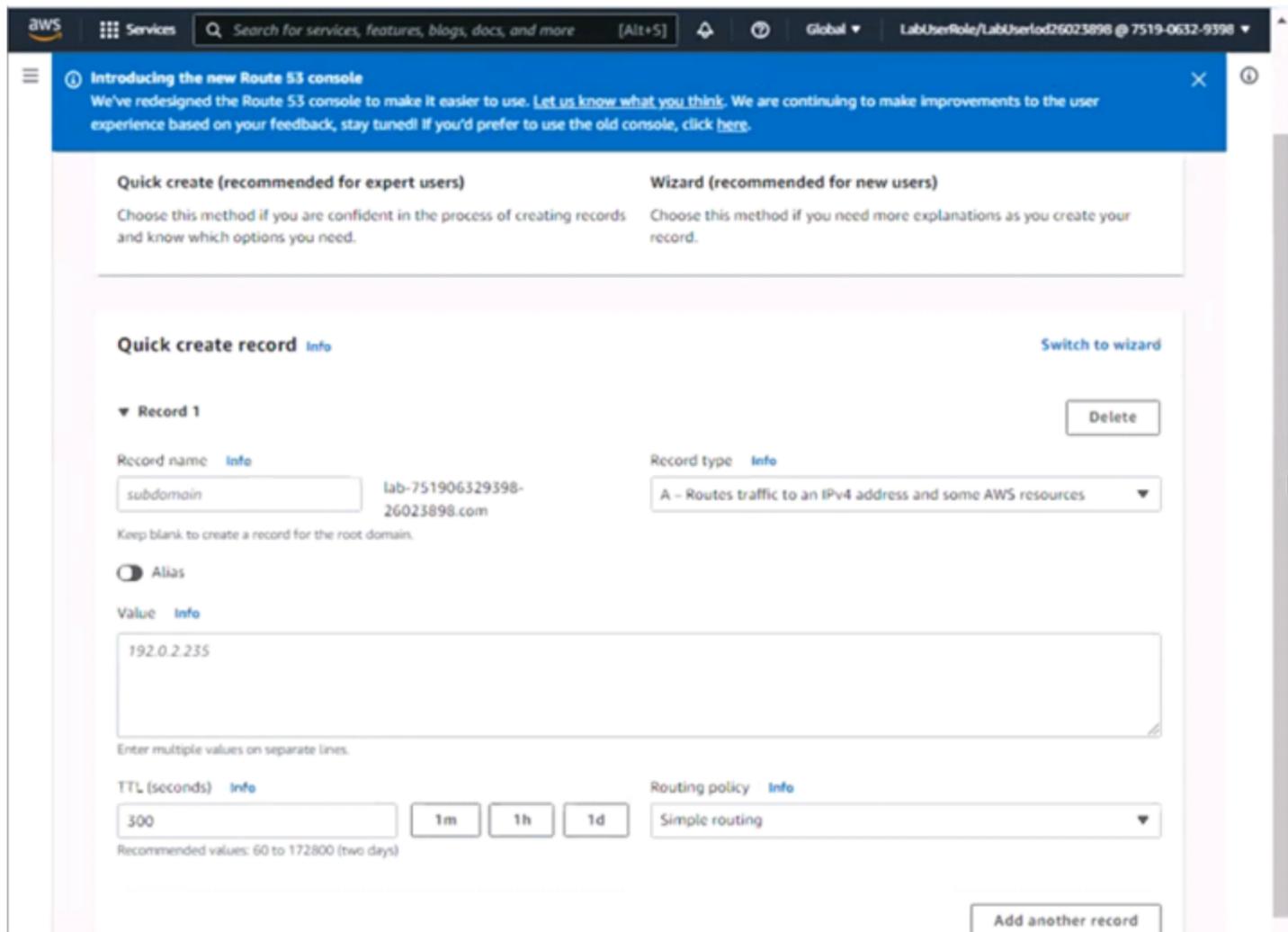


Graphical user interface, application, Teams Description automatically generated

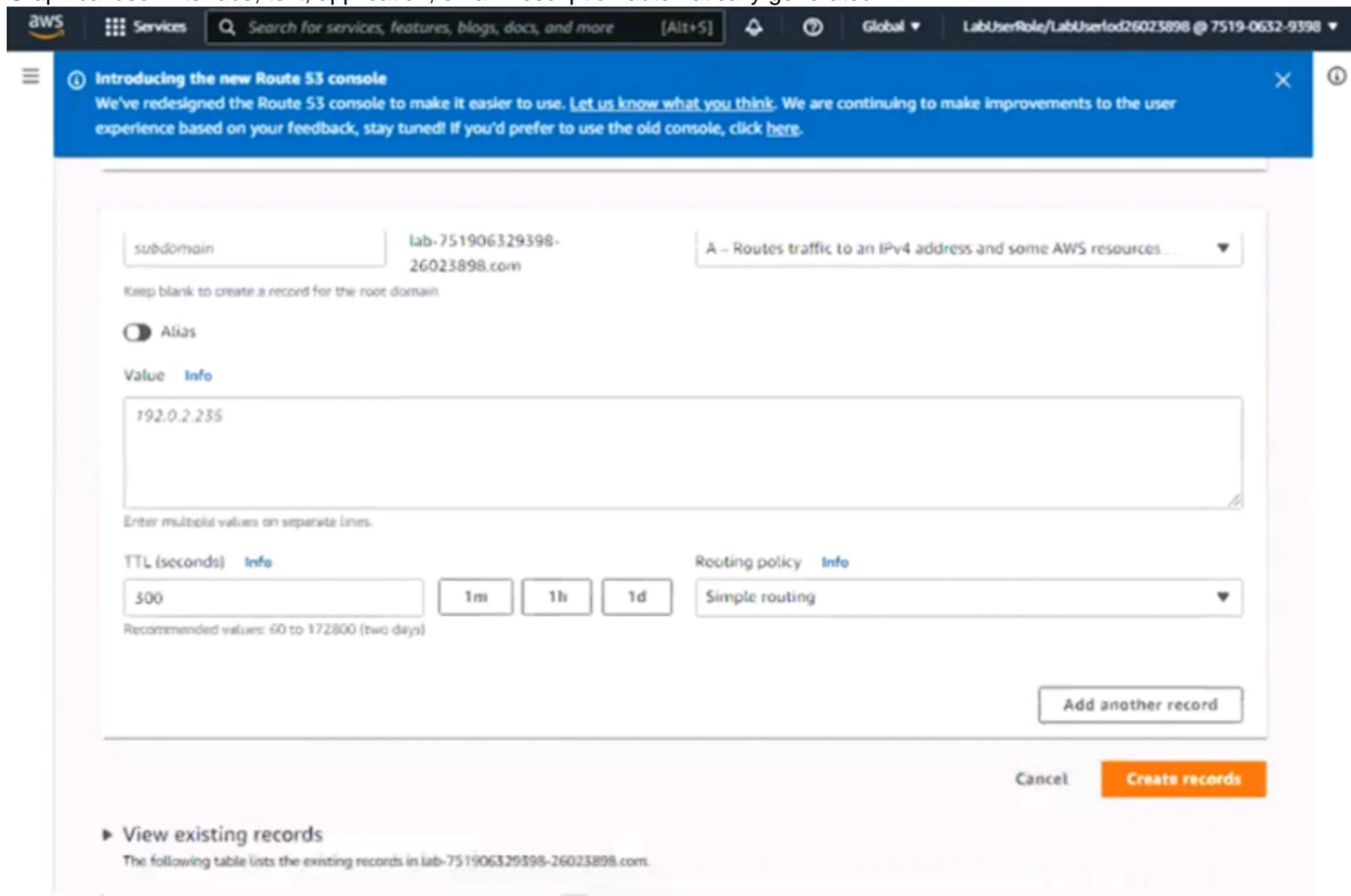


Graphical user interface, text, application Description automatically generated





Graphical user interface, text, application, email Description automatically generated



Graphical user interface, text, application Description automatically generated

**Quick create record** [Info](#)
[Switch to wizard](#)

▼ Record 1
Delete

Record name [Info](#)

Record type [Info](#)

Keep blank to create a record for the root domain.

Alias

Route traffic to [Info](#)

Alias to another record in this hosted zone

US East (N. Virginia)

An alias to a CloudFront distribution and another record in the same hosted zone are global and available only in US East (N. Virginia).

Alias hosted zone ID: Z09119752YCYFLS823AF

Routing policy [Info](#)

Failover record type

Health check ID - optional [Info](#)

Evaluate target health

 Yes

Record ID [Info](#)

Add another record

make improvements to the user experience based on your feedback, stay tuned! if you'd prefer to use the old console, click [here](#).

Route 53 > Hosted zones > lab-751906329398-26023898.com > Create record

▼ Record creation method

**Quick create (recommended for expert users)**

Choose this method if you are confident in the process of creating records and know which options you need.

**Wizard (recommended for new users)**

Choose this method if you need more explanations as you create your record.

**Quick create record** [Info](#)
[Switch to wizard](#)

▼ Record 1
Delete

Record name [Info](#)

Record type [Info](#)

Keep blank to create a record for the root domain.

Alias

Route traffic to [Info](#)

Alias to another record in this hosted zone

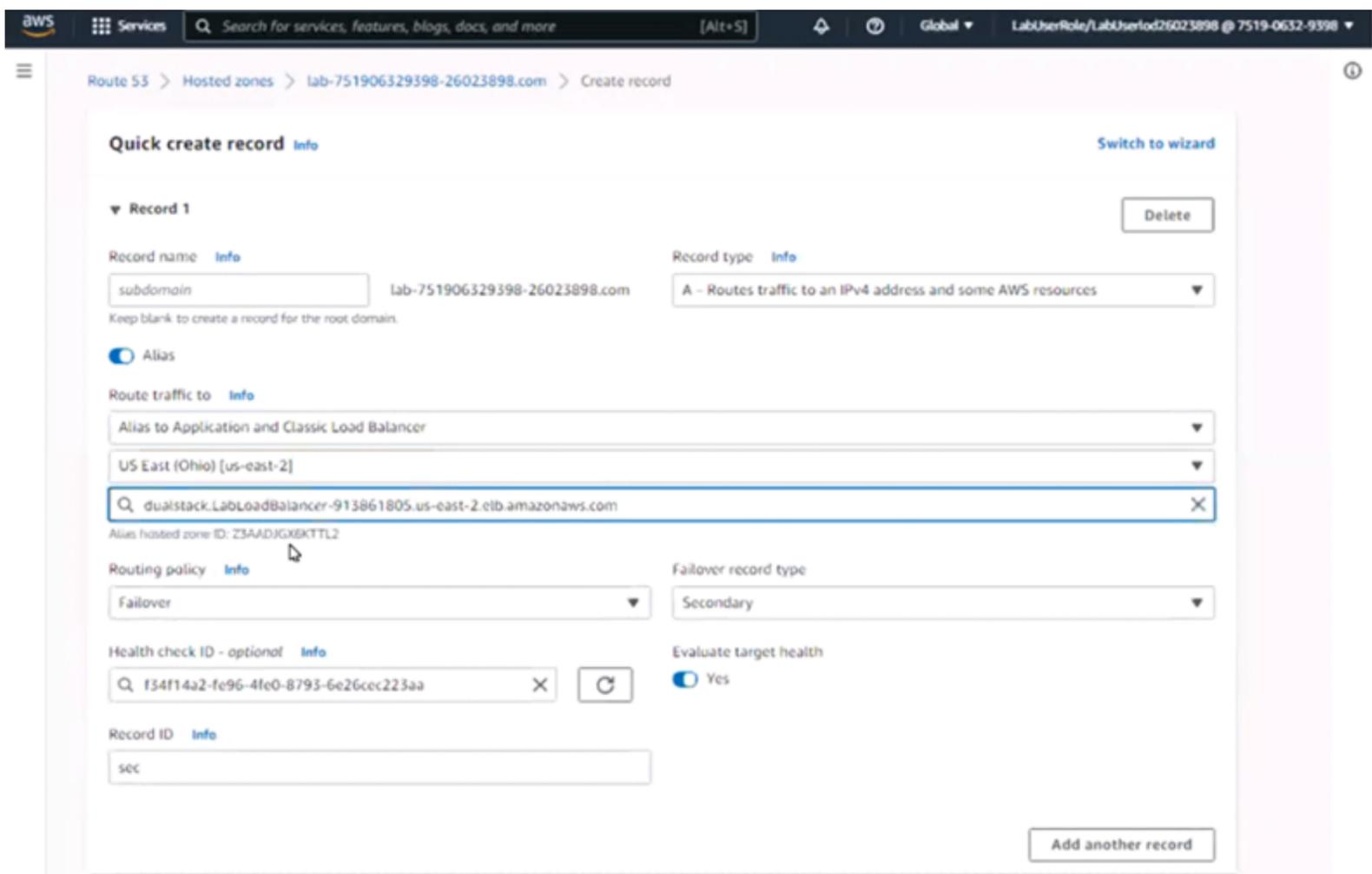
US East (N. Virginia)

An alias to a CloudFront distribution and another record in the same hosted zone are global and available only in US East (N. Virginia).

Alias hosted zone ID: Z09119752YCYFLS823AF

When you create records that have a routing policy other than simple, enter a value that uniquely identifies each record that has the same name and type. For example, you might assign a date/time stamp or a sequential counter.

[Learn more](#) [Working with records](#)



**NEW QUESTION 230**

- (Exam Topic 2)

You need to update an existing AWS CloudFormation stack. If needed, a copy to the CloudFormation template is available in an Amazon S3 bucket named cloudformation-bucket

- \* 1. Use the us-east-2 Region for all resources.
- \* 2. Unless specified below, use the default configuration settings.
- \* 3. update the Amazon EC2 instance named Devinstance by making the following changes to the stack named 1700182:
  - \* a) Change the EC2 instance type to us-east-t2.nano.
  - \* b) Allow SSH to connect to the EC2 instance from the IP address range 192.168.100.0/30.
  - \* c) Replace the instance profile IAM role with lamRoleB.
- \* 4. Deploy the changes by updating the stack using the CFServiceR01e role.
- \* 5. Edit the stack options to prevent accidental deletion.
- \* 6. Using the output from the stack, enter the value of the ProdInstanceid in the text box below:

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Here are the steps to update an existing AWS CloudFormation stack:

- Log in to the AWS Management Console and navigate to the CloudFormation service in the us-east-2 Region.
- Find the existing stack named 1700182 and click on it.
- Click on the "Update" button.
- Choose "Replace current template" and upload the updated CloudFormation template from the Amazon S3 bucket named "cloudformation-bucket"
- In the "Parameter" section, update the EC2 instance type to us-east-t2.nano and add the IP address range 192.168.100.0/30 for SSH access.
- Replace the instance profile IAM role with lamRoleB.
- In the "Capabilities" section, check the checkbox for "IAM Resources"
- Choose the role CFServiceR01e and click on "Update Stack"
- Wait for the stack to be updated.
- Once the update is complete, navigate to the stack and click on the "Stack options" button, and select "Prevent updates to prevent accidental deletion"
- To get the value of the ProdInstanceid , navigate to the "Outputs" tab in the CloudFormation stack and find the key "ProdInstanceid". The value corresponding to it is the value that you need to enter in the text box below.

Note:

- You can use AWS CloudFormation to update an existing stack.
- You can use the AWS CloudFormation service role to deploy updates.  
You can refer to the AWS CloudFormation documentation for more information on how to update and manage stacks: <https://aws.amazon.com/cloudformation/>

**NEW QUESTION 235**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your SOA-C02 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/SOA-C02-dumps.html>