

Exam Questions AWS-Certified-SysOps-Administrator-Associate

Amazon AWS Certified SysOps Administrator - Associate

<https://www.2passeasy.com/dumps/AWS-Certified-SysOps-Administrator-Associate/>



NEW QUESTION 1

- (Exam Topic 1)

A company has a mobile app that uses Amazon S3 to store images. The images are popular for a week, and then the number of access requests decreases over time. The images must be highly available and must be immediately accessible upon request. A SysOps administrator must reduce S3 storage costs for the company. Which solution will meet these requirements MOST cost-effectively?

- A. Create an S3 Lifecycle policy to transition the images to S3 Glacier after 7 days
- B. Create an S3 Lifecycle policy to transition the images to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 7 days
- C. Create an S3 Lifecycle policy to transition the images to S3 Standard after 7 days
- D. Create an S3 Lifecycle policy to transition the images to S3 Standard-Infrequent Access (S3 Standard-IA) after 7 days

Answer: D

NEW QUESTION 2

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 3

- (Exam Topic 1)

A team of on-call engineers frequently needs to connect to Amazon EC2 instances in a private subnet to troubleshoot and run commands. The instances use either the latest AWS-provided Windows Amazon Machine Images (AMIs) or Amazon Linux AMIs.

The team has an existing IAM role for authorization. A SysOps administrator must provide the team with access to the instances by granting IAM permissions to this

Which solution will meet this requirement?

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

Answer: A

NEW QUESTION 4

- (Exam Topic 1)

A company wants to create an automated solution for all accounts managed by AWS Organizations to detect any security groups that have `0.0.0.0/0` as the source address for inbound traffic. The company also wants to automatically remediate any noncompliant security groups by restricting access to a specific CIDR block that corresponds with the company's intranet.

- A. Create an AWS Config rule to detect noncompliant security groups.
- B. Set up automatic remediation to change the `0.0.0.0/0` source address to the approved CIDR block.
- C. Create an IAM policy to deny the creation of security groups that have `0.0.0.0/0` as the source address. Attach this IAM policy to every user in the company.
- D. Create an AWS Lambda function to inspect new and existing security groups, check for a noncompliant `0.0.0.0/0` source address, and change the source address to the approved CIDR block.
- E. Create a service control policy (SCP) for the organizational unit (OU) to deny the creation of security groups that have the `0.0.0.0/0` source address.
- F. Set up automatic remediation to change the `0.0.0.0/0` source address to the approved CIDR block.

Answer: A

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 company creates a new member account by using AWS Organizations. A SysOps administrator needs to add AWS Business Support to the new account. Which combination of steps must the SysOps administrator take to meet this requirement? (Select TWO.)

- A. Sign in to the new account by using 1AM credential
- B. Change the support plan.
- C. Sign in to the new account by using root user credential
- D. Change the support plan.
- E. Use the AWS Support API to change the support plan.
- F. Reset the password of the account root user.
- G. Create an IAM user that has administrator privileges in the new account.

Answer: BE

NEW QUESTION 7

- (Exam Topic 1)

A SysOps administrator is reviewing VPC Flow Logs to troubleshoot connectivity issues in a VPC. While reviewing the logs the SysOps administrator notices that rejected traffic is not listed.

What should the SysOps administrator do to ensure that all traffic is logged?

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

Answer: A

NEW QUESTION 8

- (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 9

- (Exam Topic 1)

A SysOps administrator has enabled AWS CloudTrail in an AWS account. If CloudTrail is disabled, it must be re-enabled immediately. What should the SysOps administrator do to meet these requirements WITHOUT writing custom code?

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

Answer: D

NEW QUESTION 10

- (Exam Topic 1)

A SysOps administrator needs to secure the credentials for an Amazon RDS database that is created by an AWS CloudFormation template. The solution must encrypt the credentials and must support automatic rotation.

Which solution will meet these requirements?

- A. Create an AWS::SecretsManager::Secret resource in the CloudFormation template
- B. Reference the credentials in the AWS::RDS::DBInstance resource by using the resolve:secretsmanager dynamic reference.
- C. Create an AWS::SecretsManager::Secret resource in the CloudFormation template
- D. Reference the credentials in the AWS::RDS::DBInstance resource by using the resolve:ssm-secure dynamic reference.
- E. Create an AWS::SSM::Parameter resource in the CloudFormation template
- F. Reference the credentials in the AWS::RDS::DBInstance resource by using the resolve:ssm dynamic reference.
- G. Create parameters for the database credentials in the CloudFormation template
- H. Use the Ref intrinsic function to provide the credentials to the AWS::RDS::DBInstance resource.

Answer: A

NEW QUESTION 10

- (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 15

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 18

- (Exam Topic 1)

While setting up an AWS managed VPN connection, a SysOps administrator creates a customer gateway resource in AWS. The customer gateway device resides in a data center with a NAT gateway in front of it. What address should be used to create the customer gateway resource?

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

Answer: D

NEW QUESTION 22

- (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 24

- (Exam Topic 1)

A company has an application that is deployed in two AWS Regions in an active-passive configuration. The application runs on Amazon EC2 instances behind an Application Load Balancer (ALB) in each Region. The instances are in an Amazon EC2 Auto Scaling group in each Region. The application uses an Amazon Route 53 hosted zone (or DNS). A SysOps administrator needs to configure automatic failover to the secondary Region. What should the SysOps administrator do to meet these requirements?

- A. Configure Route 53 alias records that point to each ALB.
- B. Choose a failover routing policy.
- C. Set Evaluate Target Health to Yes.
- D. Configure CNAME records that point to each ALB.
- E. Choose a failover routing policy.
- F. Set Evaluate Target Health to Yes.
- G. Configure Elastic Load Balancing (ELB) health checks for the Auto Scaling group.
- H. Add a target group to the ALB in the primary Region.
- I. Include the EC2 instances in the secondary Region as targets.
- J. Configure EC2 health checks for the Auto Scaling group.
- K. Add a target group to the ALB in the primary Region.
- L. Include the EC2 instances in the secondary Region as targets.

Answer: A

NEW QUESTION 27

- (Exam Topic 1)

A SysOps administrator applies the following policy to an AWS CloudFormation stack:

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "Update:*",
      "Principal": "*",
      "Resource": ["LogicalResourceId/Production*"]
    },
    {
      "Effect": "Allow",
      "Action": "Update:*",
      "Principal": "*",
      "Resource": "*"
    }
  ]
}
```

What is the result of this policy?

- A. Users that assume an IAM role with a logical ID that begins with "Production" are prevented from running the update-stack command.
- B. Users can update all resources in the stack except for resources that have a logical ID that begins with "Production".
- C. Users can update all resources in the stack except for resources that have an attribute that begins with "Production".
- D. Users in an IAM group with a logical ID that begins with "Production" are prevented from running the update-stack command.

Answer: B

NEW QUESTION 32

- (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 37

- (Exam Topic 1)

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

Which parameters should be specified to accomplish this in the MOST efficient manner?

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

Answer: C

NEW QUESTION 39

- (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 40

- (Exam Topic 1)

A SysOps administrator needs to delete an AWS CloudFormation stack that is no longer in use. The CloudFormation stack is in the DELETE_FAILED state. The SysOps administrator has validated the permissions that are required to delete the Cloud Formation stack.

- A. The configured timeout to delete the stack was too low for the delete operation to complete.
- B. The stack contains nested stacks that must be manually deleted first.
- C. The stack was deployed with the -disable rollback option.
- D. There are additional resources associated with a security group in the stack
- E. There are Amazon S3 buckets that still contain objects in the stack.

Answer: DE

NEW QUESTION 41

- (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 44

- (Exam Topic 1)

A web application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Auto Scaling group across multiple Availability Zones. A SysOps administrator notices that some of these EC2 instances show up as healthy in the Auto Scaling group but show up as unhealthy in the ALB target group.

What is a possible reason for this issue?

- A. Security groups are not allowing traffic between the ALB and the failing EC2 instances
- B. The Auto Scaling group health check is configured for EC2 status checks
- C. The EC2 instances are failing to launch and failing EC2 status checks.
- D. The target group health check is configured with an incorrect port or path

Answer: D

NEW QUESTION 48

- (Exam Topic 1)

A SysOps administrator must ensure that a company's Amazon EC2 instances auto scale as expected The SysOps administrator configures an Amazon EC2 Auto Scaling Lifecycle hook to send an event to Amazon EventBridge (Amazon CloudWatch Events), which then invokes an AWS Lambda function to configure the EC2 instances When the configuration is complete, the Lambda function calls the complete Lifecycle-action event to put the EC2 instances into service. In testing, the SysOps administrator discovers that the Lambda function is not invoked when the EC2 instances auto scale.

What should the SysOps administrator do to resolve this issue?

- A. Add a permission to the Lambda function so that it can be invoked by the EventBridge (CloudWatch Events) rule.
- B. Change the lifecycle hook action to CONTINUE if the lifecycle hook experiences a failure or timeout.
- C. Configure a retry policy in the EventBridge (CloudWatch Events) rule to retry the Lambda function invocation upon failure.
- D. Update the Lambda function execution role so that it has permission to call the complete lifecycle-action event

Answer: D

NEW QUESTION 52

- (Exam Topic 1)

A company is using Amazon Elastic File System (Amazon EFS) to share a file system among several Amazon EC2 instances. As usage increases, users report that file retrieval from the EFS file system is slower than normal.

Which action should a SysOps administrator take to improve the performance of the file system?

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

Answer: A

NEW QUESTION 56

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 57

- (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
- 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 62

- (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 64

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 67

- (Exam Topic 1)

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

- A. Create an Application Load Balancer that has one HTTPS listener on port 80. Attach an SSL/TLS certificate to listener port 80. Create a rule to redirect requests from HTTP to HTTPS.
- B. Create an Application Load Balancer that has one HTTP listener on port 80 and one HTTPS protocol listener on port 443. Attach an SSL/TLS certificate to listener port 443. Create a rule to redirect requests from port 80 to port 443.
- C. Create an Application Load Balancer that has two TCP listeners on port 80 and port 443. Attach an SSL/TLS certificate to listener port 443. Create a rule to redirect requests from port 80 to port 443.
- D. Create a Network Load Balancer that has two TCP listeners on port 80 and port 443. Attach an SSL/TLS certificate to listener port 443. Create a rule to redirect requests from port 80 to port 443.

Answer: B

NEW QUESTION 71

- (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 73

- (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 78

- (Exam Topic 1)

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

What is the process to rotate the key?

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

Answer: B

NEW QUESTION 83

- (Exam Topic 1)

A company runs its infrastructure on Amazon EC2 instances that run in an Auto Scaling group. Recently, the company promoted faulty code to the entire EC2 fleet. This faulty code caused the Auto Scaling group to scale the instances before any of the application logs could be retrieved.

What should a SysOps administrator do to retain the application logs after instances are terminated?

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

Answer: B

NEW QUESTION 84

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

Answer: C

Explanation:

<https://aws.amazon.com/s3/storage-classes/>

NEW QUESTION 87

- (Exam Topic 1)

A SysOps administrator must manage the security of an AWS account. Recently, an IAM user's access key was mistakenly uploaded to a public code repository. The SysOps administrator must identify anything that was changed by using this access key.

- A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to send all IAM events to an AWS Lambda function for analysis.
- B. Query Amazon EC2 logs by using Amazon CloudWatch Logs Insights for all events related to the compromised access key within the suspected timeframe.
- C. Search AWS CloudTrail event history for all events initiated with the compromised access key within the suspected timeframe.

D. Search VPC Flow Logs for all events initiated with the compromised access key within the suspected Timeframe.

Answer: C

NEW QUESTION 89

- (Exam Topic 1)

A company uses an Amazon Elastic File System (Amazon EFS) file system to share files across many Linux Amazon EC2 instances. A SysOps administrator notices that the file system's PercentIOLimit metric is consistently at 100% for 15 minutes or longer. The SysOps administrator also notices that the application that reads and writes to that file system is performing poorly. The application requires high throughput and IOPS while accessing the file system. What should the SysOps administrator do to remediate the consistently high PercentIOLimit metric?

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

Answer: A

Explanation:

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

NEW QUESTION 94

- (Exam Topic 1)

A company is storing media content in an Amazon S3 bucket and uses Amazon CloudFront to distribute the content to its users. Due to licensing terms, the company is not authorized to distribute the content in some countries. A SysOps administrator must restrict access to certain countries. What is the MOST operationally efficient solution that meets these requirements?

- A. Configure the S3 bucket policy to deny the GetObject operation based on the S3:LocationConstraint condition.
- B. Create a secondary origin access identity (OAI). Configure the S3 bucket policy to prevent access from unauthorized countries.
- C. Enable the geo restriction feature in the CloudFront distribution to prevent access from unauthorized countries.
- D. Update the application to generate signed CloudFront URLs only for IP addresses in authorized countries.

Answer: C

NEW QUESTION 99

- (Exam Topic 1)

A company has an Amazon CloudFront distribution that uses an Amazon S3 bucket as its origin. During a review of the access logs, the company determines that some requests are going directly to the S3 bucket by using the website hosting endpoint. A SysOps administrator must secure the S3 bucket to allow requests only from CloudFront.

What should the SysOps administrator do to meet this requirement?

- A. Create an origin access identity (OAI) in CloudFront
- B. Associate the OAI with the distribution
- C. Remove access to and from other principals in the S3 bucket policy
- D. Update the S3 bucket policy to allow access only from the OAI.
- E. Create an origin access identity (OAI) in CloudFront
- F. Associate the OAI with the distribution
- G. Update the S3 bucket policy to allow access only from the OAI
- H. Create a new origin, and specify the S3 bucket as the new origin
- I. Update the distribution behavior to use the new origin
- J. Remove the existing origin.
- K. Create an origin access identity (OAI) in CloudFront
- L. Associate the OAI with the distribution
- M. Update the S3 bucket policy to allow access only from the OAI
- N. Disable website hosting
- O. Create a new origin, and specify the S3 bucket as the new origin
- P. Update the distribution behavior to use the new origin
- Q. Remove the existing origin.
- R. Update the S3 bucket policy to allow access only from the CloudFront distribution
- S. Remove access to and from other principals in the S3 bucket policy
- T. Disable website hosting
- . Create a new origin, and specify the S3 bucket as the new origin
- . Update the distribution behavior to use the new origin
- . Remove the existing origin.

Answer: A

NEW QUESTION 103

- (Exam Topic 1)

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

- A. Connect a large Amazon EBS volume to multiple instances and schedule snapshots.
- B. Deploy Amazon EFS in the VPC and create mount targets in multiple subnets.

- C. Launch an EC2 instance and share data using SMB/CIFS or NFS.
- D. Deploy an AWS Storage Gateway cached volume on Amazon EC2.

Answer: B

NEW QUESTION 105

- (Exam Topic 1)

A company has a public website that recently experienced problems. Some links led to missing webpages, and other links rendered incorrect webpages. The application infrastructure was running properly, and all the provisioned resources were healthy. Application logs and dashboards did not show any errors, and no monitoring alarms were raised. Systems administrators were not aware of any problems until end users reported the issues. The company needs to proactively monitor the website for such issues in the future and must implement a solution as soon as possible. Which solution will meet these requirements with the LEAST operational overhead?

- A. Rewrite the application to surface a custom error to the application log when issues occur. Automatically parse logs for error
- B. Create an Amazon CloudWatch alarm to provide alerts when issues are detected.
- C. Create an AWS Lambda function to test the website
- D. Configure the Lambda function to emit an Amazon CloudWatch custom metric when errors are detected
- E. Configure a CloudWatch alarm to provide alerts when issues are detected.
- F. Create an Amazon CloudWatch Synthetic canary
- G. Use the CloudWatch Synthetic Recorder plugin to generate the script for the canary run
- H. Configure the canary in line with requirements
- I. Create an alarm to provide alerts when issues are detected.

Answer: A

NEW QUESTION 108

- (Exam Topic 1)

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

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

Answer: B

Explanation:

<https://aws.amazon.com/blogs/compute/using-amazon-rds-proxy-with-aws-lambda/>

RDS Proxy acts as an intermediary between your application and an RDS database. RDS Proxy establishes and manages the necessary connection pools to your database so that your application creates fewer database connections. Your Lambda functions interact with RDS Proxy instead of your database instance. It handles the connection pooling necessary for scaling many simultaneous connections created by concurrent Lambda functions. This allows your Lambda applications to reuse existing connections, rather than creating new connections for every function invocation.

Check "Database proxy for Amazon RDS" section in the link to see how RDS proxy helps Lambda handle huge connections to RDS MySQL.

<https://aws.amazon.com/blogs/compute/using-amazon-rds-proxy-with-aws-lambda/>

NEW QUESTION 112

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 116

- (Exam Topic 1)

A company has a high-performance Windows workload. The workload requires a storage volume that provides consistent performance of 10,000 KDPS. The company does not want to pay for additional unneeded capacity to achieve this performance. Which solution will meet these requirements with the LEAST cost?

- A. Use a Provisioned IOPS SSD (io1) Amazon Elastic Block Store (Amazon EBS) volume that is configured with 10,000 provisioned IOPS.
- B. Use a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume that is configured with 10,000 provisioned IOPS.
- C. Use an Amazon Elastic File System (Amazon EFS) file system with Max I/O mode.
- D. Use an Amazon FSx for Windows File Server file system that is configured with 10,000 IOPS.

Answer: A

NEW QUESTION 117

- (Exam Topic 1)

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

How should a SysOps administrator create a new record for the subdomain in Route 53?

- A. Create a CNAME record
- B. Enter static.cloudfront.net as the record name
- C. Enter the CloudFront distribution's public IP address as the value.
- D. Create an A record
- E. Enter static.example.com as the record name
- F. Enter the CloudFront distribution's private IP address as the value.
- G. Create an A record
- H. Enter static.cloudfront.net as the record name
- I. Enter the CloudFront distribution's ID as an alias target.
- J. Create an A record
- K. Enter static.example.com as the record name
- L. Enter the CloudFront distribution's domain name as an alias target.

Answer: D

Explanation:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-cloudfront-distribution.html>

NEW QUESTION 120

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

Answer: B

NEW QUESTION 125

- (Exam Topic 1)

A company uploaded its website files to an Amazon S3 bucket that has S3 Versioning enabled. The company uses an Amazon CloudFront distribution with the S3 bucket as the origin. The company recently modified the files, but the object names remained the same. Users report that old content is still appearing on the website.

How should a SysOps administrator remediate this issue?

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

Answer: A

NEW QUESTION 127

- (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 metric
- 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 group
- 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 131

- (Exam Topic 1)

A company wants to archive sensitive data on Amazon S3 Glacier. The company's regulatory and compliance requirements do not allow any modifications to the data by any account.

Which solution meets these requirements?

- A. Attach a vault lock policy to an S3 Glacier vault that contains the archived data

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

Answer: B

NEW QUESTION 134

- (Exam Topic 1)

A company is migrating its production file server to AWS. All data that is stored on the file server must remain accessible if an Availability Zone becomes unavailable or when system maintenance is performed. Users must be able to interact with the file server through the SMB protocol. Users also must have the ability to manage file permissions by using Windows ACLs.

Which solution will meet these requirements?

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

Answer: B

Explanation:

<https://aws.amazon.com/fsx/windows/>

NEW QUESTION 135

- (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 136

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 140

- (Exam Topic 1)

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

What should a SysOps administrator do to meet the compliance requirement?

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

Answer: B

NEW QUESTION 144

- (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 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 151

- (Exam Topic 1)

A SysOps administrator is using Amazon EC2 instances to host an application. The SysOps administrator needs to grant permissions for the application to access an Amazon DynamoDB table.

Which solution will meet this requirement?

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

Answer: D

NEW QUESTION 153

- (Exam Topic 1)

A company needs to upload gigabytes of files every day. The company needs to achieve higher throughput and upload speeds to Amazon S3. Which action should a SysOps administrator take to meet this requirement?

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

Answer: D

Explanation:

Enable Amazon S3 Transfer Acceleration. Amazon S3 Transfer Acceleration can provide fast and secure transfers over long distances between your client and Amazon S3. Transfer Acceleration uses Amazon CloudFront's globally distributed edge locations.

<https://aws.amazon.com/premiumsupport/knowledge-center/s3-upload-large-files/>

NEW QUESTION 154

- (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 Replic
- 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 159

- (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 164

- (Exam Topic 1)

A company maintains a large set of sensitive data in an Amazon S3 bucket. The company's security team asks a SysOps administrator to help verify that all current objects in the S3 bucket are encrypted.

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

- A. Create a script that runs against the S3 bucket and outputs the status of each object.
- B. Create an S3 Inventory configuration on the S3 bucket. Induce the appropriate status fields.
- C. Provide the security team with an IAM user that has read access to the S3 bucket.
- D. Use the AWS CLI to output a list of all objects in the S3 bucket.

Answer: D

NEW QUESTION 165

- (Exam Topic 1)

A company's backend infrastructure contains an Amazon EC2 instance in a private subnet. The private subnet has a route to the internet through a NAT gateway in a public subnet. The instance must allow connectivity to a secure web server on the internet to retrieve data at regular intervals.

The client software times out with an error message that indicates that the client software could not establish the TCP connection.

What should a SysOps administrator do to resolve this error?

- A. Add an inbound rule to the security group for the EC2 instance with the following parameters: Type - HTTP, Source - 0.0.0.0/0.
- B. Add an inbound rule to the security group for the EC2 instance with the following parameters: Type - HTTPS, Source - 0.0.0.0/0.
- C. Add an outbound rule to the security group for the EC2 instance with the following parameters: Type - HTTP, Destination - 0.0.0.0/0.
- D. Add an outbound rule to the security group for the EC2 instance with the following parameters: Type - HTTP
- E. Destination - 0.0.0.0/0.

Answer: D

NEW QUESTION 170

- (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 173

- (Exam Topic 1)

A company has an AWS CloudFormation template that creates an Amazon S3 bucket. A user authenticates to the corporate AWS account with their Active Directory credentials and attempts to deploy the CloudFormation template. However, the stack creation fails. Which factors could cause this failure? (Select TWO.)

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

Answer: AC

NEW QUESTION 178

- (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 181

- (Exam Topic 1)

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

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

Answer: D

Explanation:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.htm>

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

NEW QUESTION 184

- (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 189

- (Exam Topic 1)

A company has an internal web application that runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group in a single Availability Zone. A SysOps administrator must make the application highly available.

Which action should the SysOps administrator take to meet this requirement?

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

Answer: C

NEW QUESTION 194

- (Exam Topic 1)

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

Which of the following is a cause of this?

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

Answer: D

NEW QUESTION 199

- (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 202

- (Exam Topic 1)

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

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

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

Answer: CD

Explanation:

"C" because Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer

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

"D" because "you can configure CloudFront to create log files that contain detailed information about every user request that CloudFront receives"

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html>

NEW QUESTION 207

- (Exam Topic 1)

A company has a stateful web application that is hosted on Amazon EC2 instances in an Auto Scaling group. The instances run behind an Application Load Balancer (ALB) that has a single target group. The ALB is configured as the origin in an Amazon CloudFront distribution. Users are reporting random logouts from the web application.

Which combination of actions should a SysOps administrator take to resolve this problem? (Select TWO.)

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

Answer: BE

Explanation:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Cookies.html>

You can configure each cache behavior to do one of the following: Forward all cookies to your origin – CloudFront includes all cookies sent by the viewer when it forwards requests to the origin. <https://docs.aws.amazon.com/elasticloadbalancing/latest/application/sticky-sessions.html>

By default, an Application Load Balancer routes each request independently to a registered target based on the chosen load-balancing algorithm.

NEW QUESTION 211

- (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 212

- (Exam Topic 1)

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

The MOST effective way to reduce latency is to relaunch the EC2 instances in:

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

Answer: C

NEW QUESTION 216

- (Exam Topic 1)

An environment consists of 100 Amazon EC2 Windows instances. The Amazon CloudWatch agent is deployed and running on all EC2 instances with a baseline configuration file to capture log files. There is a new requirement to capture the DHCP log files that exist on 50 of the instances.

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

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

Answer: A

NEW QUESTION 218

- (Exam Topic 1)

A company wants to use only IPv6 for all its Amazon EC2 instances. The EC2 instances must not be accessible from the internet, but the EC2 instances must be able to access the internet. The company creates a dual-stack VPC and IPv6-only subnets.

How should a SysOps administrator configure the VPC to meet these requirements?

- A. Create and attach a NAT gateway.
- B. Create a custom route table that includes an entry to point all IPv6 traffic to the NAT gateway.
- C. Attach the custom route table to the IPv6-only subnets.
- D. Create and attach an internet gateway.
- E. Create a custom route table that includes an entry to point all IPv6 traffic to the internet gateway.
- F. Attach the custom route table to the IPv6-only subnets.
- G. Create and attach an egress-only internet gateway.
- H. Create a custom route table that includes an entry to point all IPv6 traffic to the egress-only internet gateway.
- I. Attach the custom route table to the IPv6-only subnets.
- J. Create and attach an internet gateway and a NAT gateway.
- K. Create a custom route table that includes an entry to point all IPv6 traffic to the internet gateway and all IPv4 traffic to the NAT gateway.
- L. Attach the custom route table to the IPv6-only subnets.

Answer: C

NEW QUESTION 223

- (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 226

- (Exam Topic 1)

A SysOps administrator configuring AWS Client VPN to connect users on a corporate network to AWS resources that are running in a VPC. According to compliance requirements, only traffic that is destined for the VPC can travel across the VPN tunnel.

How should the SysOps administrator configure Client VPN to meet these requirements?

- A. Associate the Client VPN endpoint with a private subnet that has an internet route through a NAT gateway.
- B. On the Client VPN endpoint, turn on the split-tunnel option.
- C. On the Client VPN endpoint, specify DNS server IP addresses.
- D. Select a private certificate to use as the identity certificate for the VPN client.

Answer: C

NEW QUESTION 228

- (Exam Topic 1)

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

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

Answer: D

Explanation:

<https://docs.aws.amazon.com/health/latest/ug/cloudwatch-events-health.html>

NEW QUESTION 230

- (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 232

- (Exam Topic 1)

A company's financial department needs to view the cost details of each project in an AWS account. A SysOps administrator must perform the initial configuration that is required to view cost for each project in Cost Explorer.

Which solution will meet this requirement?

- A. Activate cost allocation tags. Add a project tag to the appropriate resources.
- B. Configure consolidated billing. Create AWS Cost and Usage Reports.
- C. Use AWS Budgets. Create AWS Budgets reports.
- D. Use cost categories to define custom groups that are based on AWS cost and usage dimensions.

Answer: A

NEW QUESTION 235

- (Exam Topic 1)

A large multinational company has a core application that runs 24 hours a day, 7 days a week on Amazon EC2 and AWS Lambda. The company uses a combination of operating systems across different AWS Regions. The company wants to achieve cost savings and wants to use a pricing model that provides the most flexibility.

What should the company do to MAXIMIZE cost savings while meeting these requirements?

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

Answer: D

NEW QUESTION 236

- (Exam Topic 1)

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

- A. Log in to the RDS console and select the encryption box to encrypt the database.
- B. Create a new encrypted Amazon EBS volume and attach it to the instance.
- C. Encrypt the standby replica in the secondary Availability Zone and promote it to the primary instance.

D. Take a snapshot of the RDS instance, copy and encrypt the snapshot and then restore to the new RDS instance

Answer: D

NEW QUESTION 237

- (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 240

- (Exam Topic 1)

A company has multiple Amazon EC2 instances that run a resource-intensive application in a development environment. A SysOps administrator is implementing a solution to stop these EC2 instances when they are not in use.

Which solution will meet this requirement?

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

Answer: B

Explanation:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/UsingAlarmActions.html#AddingStopActi>

NEW QUESTION 244

- (Exam Topic 1)

A company uses Amazon S3 to aggregate raw video footage from various media teams across the US. The company recently expanded into new geographies in Europe and Australia. The technical teams located in Europe and Australia reported delays when uploading large video tiles into the destination S3 bucket in the United States.

What are the MOST cost-effective ways to increase upload speeds into the S3 bucket? (Select TWO.)

- A. Create multiple AWS Direct Connect connections between AWS and branch offices in Europe and Australia for file uploads into the destination S3 bucket
- B. Create multiple AWS Site-to-Site VPN connections between AWS and branch offices in Europe and Australia for file uploads into the destination S3 bucket.
- C. Use Amazon S3 Transfer Acceleration for file uploads into the destination S3 bucket.
- D. Use AWS Global Accelerator for file uploads into the destination S3 bucket from the branch offices in Europe and Australia.
- E. Use multipart uploads for file uploads into the destination S3 bucket from the branch offices in Europe and Australia.

Answer: CE

NEW QUESTION 249

- (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? (Select TWO.) Create a Systems Manager Distributor package for the third-party agent.

- A. Make sure that Systems Manager Inventory is configured
- B. If Systems Manager Inventory is not configured, set up a new inventory for 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 package
- 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 document
- F. Populate the details of the third-party agent package
- 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 OpsItem
- I. Create a maintenance window that is specific to the package deployment. Configure the maintenance window to cover 24 hours a day.

Answer: D

NEW QUESTION 252

- (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 256

- (Exam Topic 1)

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

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

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

Answer: B

NEW QUESTION 259

- (Exam Topic 1)

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

Which solution will meet these requirements MOST cost-effectively?

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

Answer: B

NEW QUESTION 260

- (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 263

- (Exam Topic 1)

An Amazon S3 Inventory report reveals that more than 1 million objects in an S3 bucket are not encrypted. These objects must be encrypted, and all future objects must be encrypted at the time they are written.

Which combination of actions should a SysOps administrator take to meet these requirements? (Select TWO)

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

Answer: BC

Explanation:

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

NEW QUESTION 268

- (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

NEW QUESTION 270

- (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 274

- (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 Plan based on the usage during the past 30 days
- D. Purchase Standard Reserved Instances by calculating the usage baseline.

Answer: C

NEW QUESTION 275

- (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.

- 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
- E. CreateStack API call
- F. Use AWS CloudFormation StackSets from the management account to deploy the template in each of the accounts

Answer: D

NEW QUESTION 280

- (Exam Topic 1)

A company uses AWS Organizations. A SysOps administrator wants to use AWS Compute Optimizer and AWS tag policies in the management account to govern all member accounts in the billing family. The SysOps administrator navigates to the AWS Organizations console but cannot activate tag policies through the management account.

What could be the reason for this issue?

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

Answer: C

NEW QUESTION 283

- (Exam Topic 1)

A new website will run on Amazon EC2 instances behind an Application Load Balancer. Amazon Route 53 will be used to manage DNS records.

What type of record should be set in Route 53 to point the website's apex domain name (for example, company.com) to the Application Load Balancer?

- A. CNAME
- B. SOA

- C. TXT
- D. ALIAS

Answer: D

NEW QUESTION 288

- (Exam Topic 1)

A company hosts its website in the us-east-1 Region. The company is preparing to deploy its website into the eu-central-1 Region. Website visitors who are located in Europe should access the website that is hosted in eu-central-1. All other visitors access the website that is hosted in us-east-1. The company uses Amazon Route 53 to manage the website's DNS records.

Which routing policy should a SysOps administrator apply to the Route 53 record set to meet these requirements?

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

Answer: A

Explanation:

geolocation "Geolocation routing lets you choose the resources that serve your traffic based on the geographic location of your users, meaning the location that DNS queries originate from. For example, you might want all queries from Europe to be routed to an ELB load balancer in the Frankfurt region."

Could be confused with geoproximity - "Geoproximity routing lets Amazon Route 53 route traffic to your resources based on the geographic location of your users and your resources. You can also optionally choose to route more traffic or less to a given resource by specifying a value, known as a bias. A bias expands or shrinks the size of the geographic region from which traffic is routed to a resource" the use case is not needed as per question.

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

NEW QUESTION 292

- (Exam Topic 1)

A company is deploying a third-party unit testing solution that is delivered as an Amazon EC2 Amazon Machine Image (AMI). All system configuration data is stored in Amazon DynamoDB. The testing results are stored in Amazon S3.

A minimum of three EC2 instances are required to operate the product. The company's testing team wants to use an additional three EC2 Instances when the Spot Instance prices are at a certain threshold. A SysOps administrator must Implement a highly available solution that provides this functionality.

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

- A. Define an Amazon EC2 Auto Scaling group by using a launch configuratio
- B. Use the provided AMI In the launch configuratio
- C. Configure three On-Demand Instances and three Spot Instance
- D. Configure a maximum Spot Instance price In the launch configuration.
- E. Define an Amazon EC2 Auto Scaling group by using a launch templat
- F. Use the provided AMI in the launch templat
- G. Configure three On-Demand Instances and three Spot Instance
- H. Configure a maximum Spot Instance price In the launch template.
- I. Define two Amazon EC2 Auto Scaling groups by using launch configuration
- J. Use the provided AMI in the launch configuration
- K. Configure three On-Demand Instances for one Auto Scaling grou
- L. Configure three Spot Instances for the other Auto Scaling grou
- M. Configure a maximum Spot Instance price in the launch configuration for the Auto Scaling group that has Spot Instances.
- N. Define two Amazon EC2 Auto Scaling groups by using launch template
- O. Use the provided AMI in the launch template
- P. Configure three On-DemandInstances for one Auto Scaling grou
- Q. Configure three Spot Instances for the other Auto Scaling group
- R. Configure a maximum Spot Instance price in the launch template for the Auto Scaling group that has Spot Instances.

Answer: C

NEW QUESTION 296

- (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 Regio
- B. Create a single start of authority (SOA) record in Route 53 that includes the IP address from each EL
- 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 Regio
- F. Create an additional A record in Route 53 that includes the ELB in us-west-2 as an alias targe
- 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 Regio
- J. Associate the new EC2 instances with the existing ELB, and configure load balancer health checks on all EC2 instance
- 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 Regio
- M. Configure EC2 health checks on all EC2 instances in each Regio
- 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

NEW QUESTION 299

- (Exam Topic 1)

A SysOps administrator is creating two AWS CloudFormation templates. The first template will create a VPC with associated resources, such as subnets, route tables, and an internet gateway. The second template will deploy application resources within the VPC that was created by the first template. The second template should refer to the resources created by the first template.

How can this be accomplished with the LEAST amount of administrative effort?

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

Answer: A

Explanation:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-stack-exports.html>

NEW QUESTION 304

- (Exam Topic 1)

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

Which configuration meets these requirements?

- A. Deploy two Auto Scaling groups in two Availability Zones with a minimum capacity of two instances in each group.
- B. Deploy an Auto Scaling group across two Availability Zones with a minimum capacity of four instances.
- C. Deploy an Auto Scaling group across three Availability Zones with a minimum capacity of four instances.
- D. Deploy an Auto Scaling group across three Availability Zones with a minimum capacity of six instances.

Answer: C

NEW QUESTION 306

- (Exam Topic 1)

A company is releasing a new static website hosted on Amazon S3. The static website hosting feature was enabled on the bucket and content was uploaded; however, upon navigating to the site, the following error message is received:

403 Forbidden - Access Denied

What change should be made to fix this error?

- A. Add a bucket policy that grants everyone read access to the bucket.
- B. Add a bucket policy that grants everyone read access to the bucket objects.
- C. Remove the default bucket policy that denies read access to the bucket.
- D. Configure cross-origin resource sharing (CORS) on the bucket.

Answer: B

NEW QUESTION 307

- (Exam Topic 1)

A SysOps administrator is required to monitor free space on Amazon EBS volumes attached to Microsoft Windows-based Amazon EC2 instances within a company's account. The administrator must be alerted to potential issues.

What should the administrator do to receive email alerts before low storage space affects EC2 instance performance?

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

Answer: C

NEW QUESTION 311

- (Exam Topic 1)

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

Which solution will securely share the AMI with the other AWS accounts?

- A. In the account where the AMI was created, create a customer master key (CMK). Modify the key policy to provide kms:DescribeKey, kms:ReEncrypt, kms>CreateGrant, and kms:Decrypt permissions to the AWS accounts that the AMI will be shared with
- B. Modify the AMI permissions to specify the AWS account numbers that the AMI will be shared with.
- C. In the account where the AMI was created, create a customer master key (CMK). Modify the key policy to provide kms:DescribeKey, kms:ReEncrypt*, kms>CreateGrant, and kms:Decrypt permissions to the AWS accounts that the AMI will be shared with
- D. Create a copy of the AMI

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

Answer: B

Explanation:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sharingamis-explicit.html>

NEW QUESTION 314

- (Exam Topic 1)

A new application runs on Amazon EC2 instances and accesses data in an Amazon RDS database instance. When fully deployed in production, the application fails. The database can be queried from a console on a bastion host. When looking at the web server logs, the following error is repeated multiple times:

*** Error Establishing a Database Connection

Which of the following may be causes of the connectivity problems? (Select TWO.)

- A. The security group for the database does not have the appropriate egress rule from the database to the web server.
- B. The certificate used by the web server is not trusted by the RDS instance.
- C. The security group for the database does not have the appropriate ingress rule from the web server to the database.
- D. The port used by the application developer does not match the port specified in the RDS configuration.
- E. The database is still being created and is not available for connectivity.

Answer: CD

NEW QUESTION 316

- (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 321

- (Exam Topic 1)

A large company is using AWS Organizations to manage hundreds of AWS accounts across multiple AWS Regions. The company has turned on AWS Config throughout the organization.

The company requires all Amazon S3 buckets to block public read access. A SysOps administrator must generate a monthly report that shows all the S3 buckets and whether they comply with this requirement.

Which combination of steps should the SysOps administrator take to collect this data? (Select TWO).

- A. Create an AWS Config aggregator in an aggregator account.
- B. Use the organization as the source. Retrieve the compliance data from the aggregator.
- C. Create an AWS Config aggregator in each account.
- D. Use an S3 bucket in an aggregator account as the destination.
- E. Retrieve the compliance data from the S3 bucket.
- F. Edit the AWS Config policy in AWS Organization.
- G. Use the organization's management account to turn on the s3-bucket-public-read-prohibited rule for the entire organization.
- H. Use the AWS Config compliance report from the organization's management account.

- I. Filter the results by resource, and select Amazon S3.
- J. Use the AWS Config API to apply the s3-bucket-public-read-prohibited rule in all accounts for all available Regions.

Answer: CD

NEW QUESTION 324

- (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 325

- (Exam Topic 1)

A SysOps administrator is deploying a test site running on Amazon EC2 instances. The application requires both incoming and outgoing connectivity to the internet.

Which combination of steps are required to provide internet connectivity to the EC2 instances? (Choose two.)

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

Answer: DE

Explanation:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html

NEW QUESTION 328

- (Exam Topic 1)

A company has an internal web application that runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group in a single Availability Zone. A SysOps administrator must make the application highly available.

Which action should the SysOps administrator take to meet this requirement?

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

Answer: C

Explanation:

"An Auto Scaling group can contain EC2 instances in one or more Availability Zones within the same Region. However, Auto Scaling groups cannot span multiple Regions". As stated in <https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-benefits.htm>

NEW QUESTION 331

- (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 333

- (Exam Topic 1)

A company is using Amazon Elastic File System (Amazon EFS) to share a file system among several Amazon EC2 instances. As usage increases, users report that file retrieval from the EFS file system is slower than normal.

Which action should a SysOps administrator take to improve the performance of the file system?

- A. Configure the file system for Provisioned Throughput.
- B. Enable encryption in transit on the file system.
- C. Identify any unused files in the file system, and remove the unused files.

D. Resize the Amazon Elastic Block Store (Amazon EBS) volume of each of the EC2 instances.

Answer: A

NEW QUESTION 338

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

Answer: B

NEW QUESTION 340

- (Exam Topic 1)

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

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

Answer: B

Explanation:

<https://aws.amazon.com/blogs/security/how-to-enable-secure-access-to-kibana-using-aws-single-sign-on/> <https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-cognito-auth.html>

NEW QUESTION 342

- (Exam Topic 2)

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

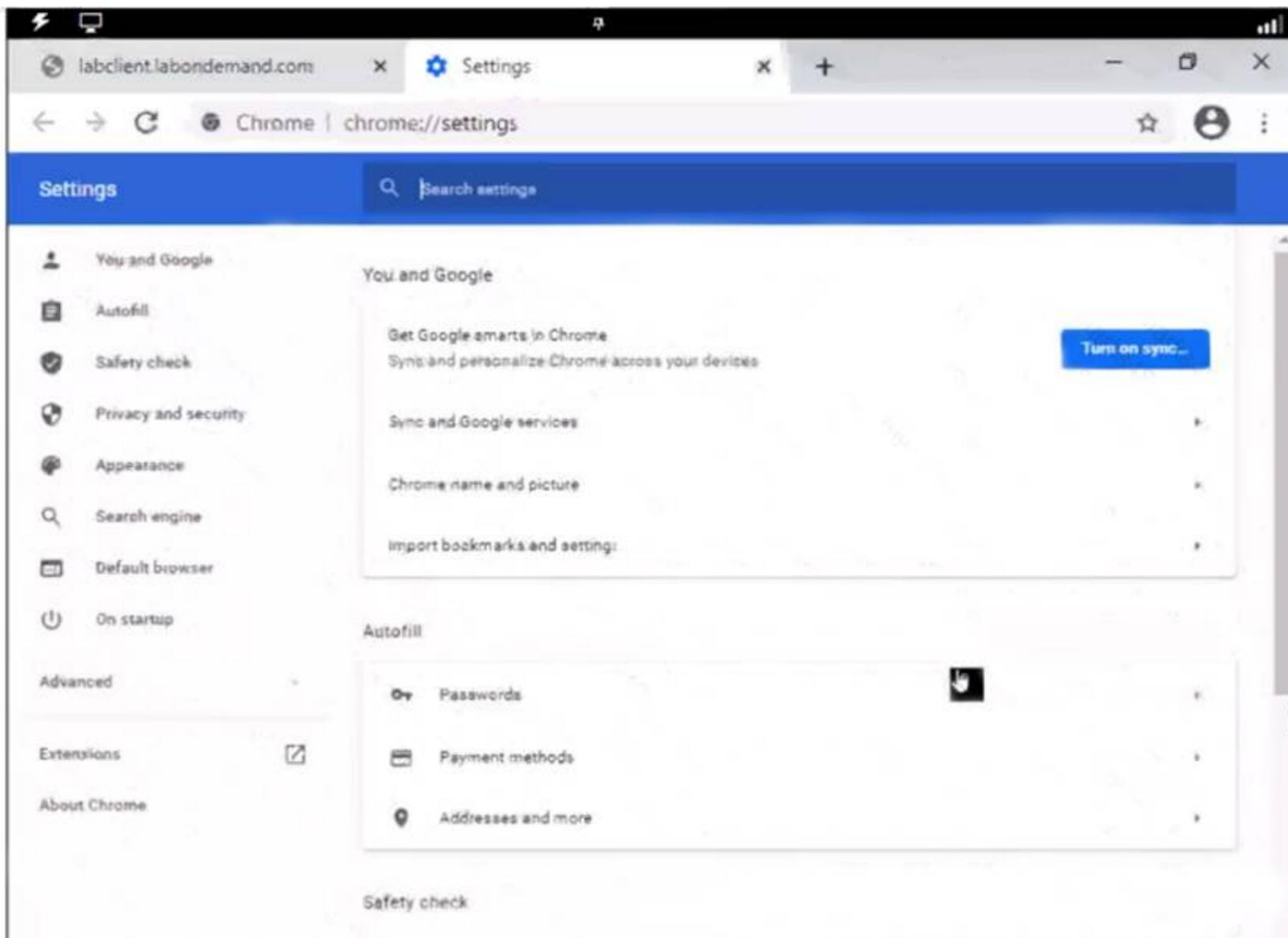
- * 1. Use the us-east-2 Region for all resources.
- * 2. Unless specified below, use the default configuration settings.
- * 3. update the Amazon EC2 instance named DevInstance by making the following changes to the stack named 1700182:
 - * a) Change the EC2 instance type to us-east-t2.nano.
 - * b) 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:

Solution as given below.

**NEW QUESTION 343**

- (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 lab751906329398-26023898.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:

Solution as given below.

Recently visited Info

No recently visited services

Explore one of these commonly visited AWS services.

[IAM](#) [EC2](#) [S3](#) [RDS](#) [Lambda](#)

[View all services](#)

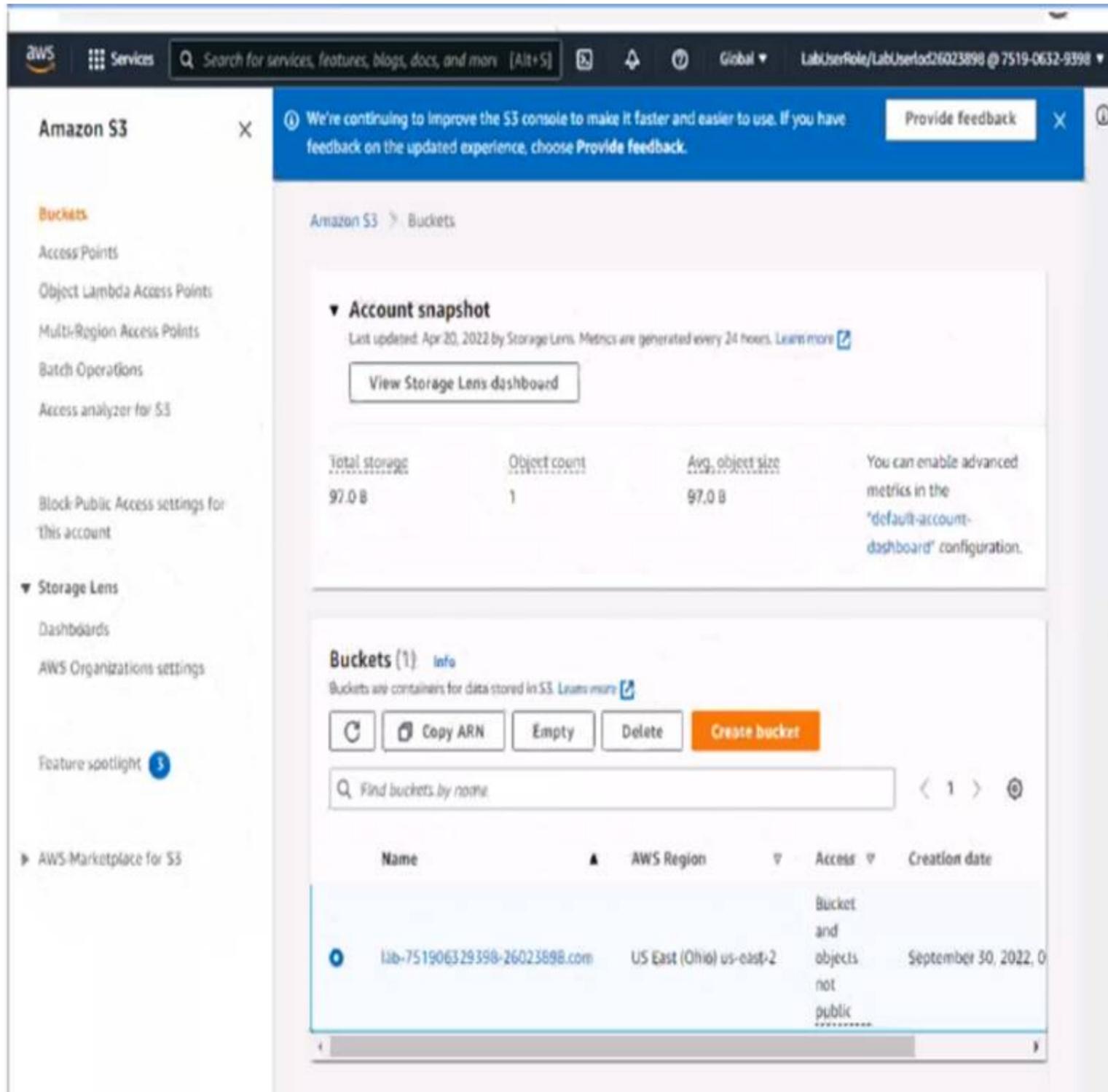
Welcome to AWS

-  **Getting started with AWS** [↗](#)
Learn the fundamentals and find valuable information to get the most out of AWS.
-  **Training and certification** [↗](#)
Learn from AWS experts and advance your skills and knowledge.
-  **What's new with AWS?** [↗](#)

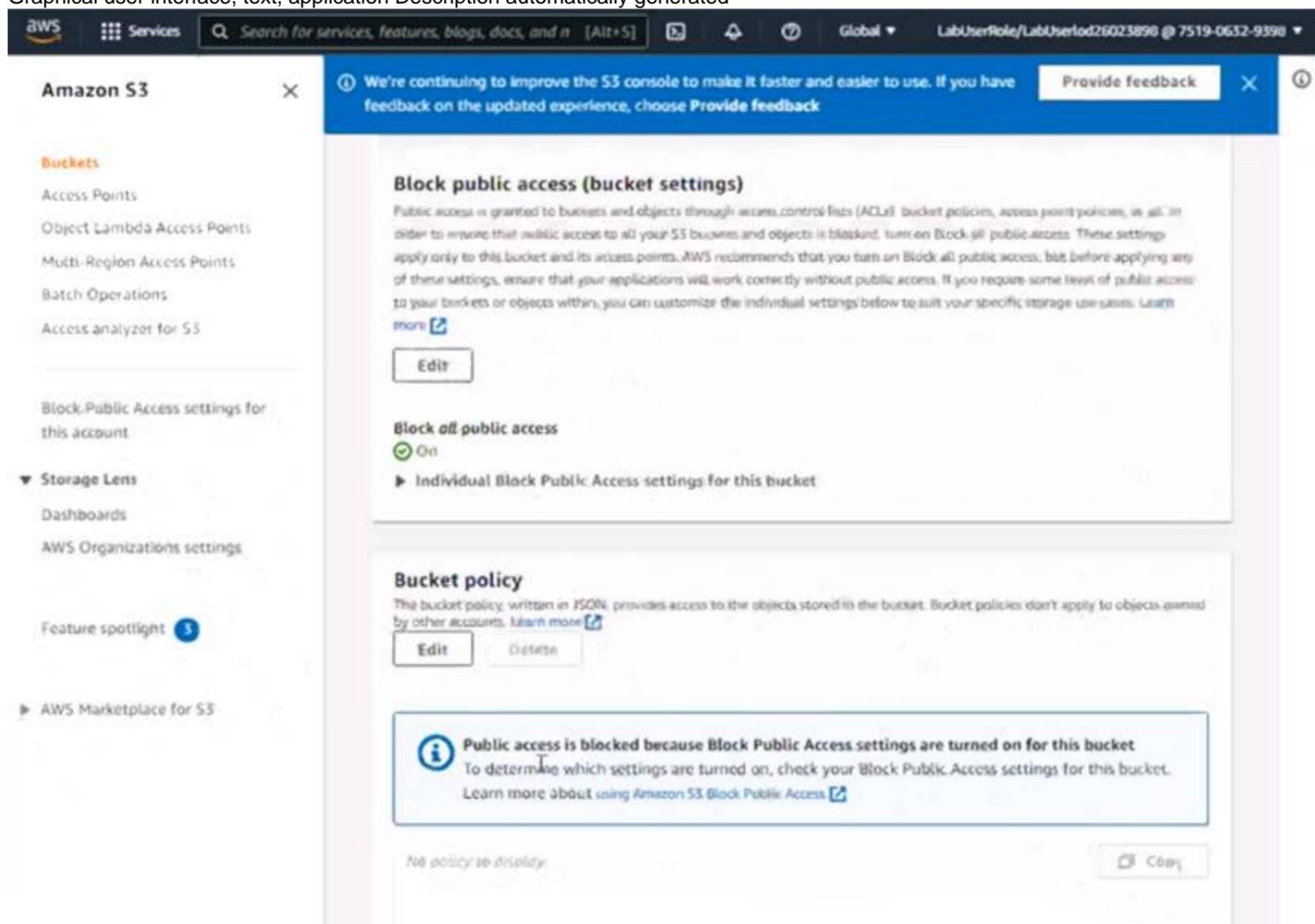
AWS Health Info

No health data

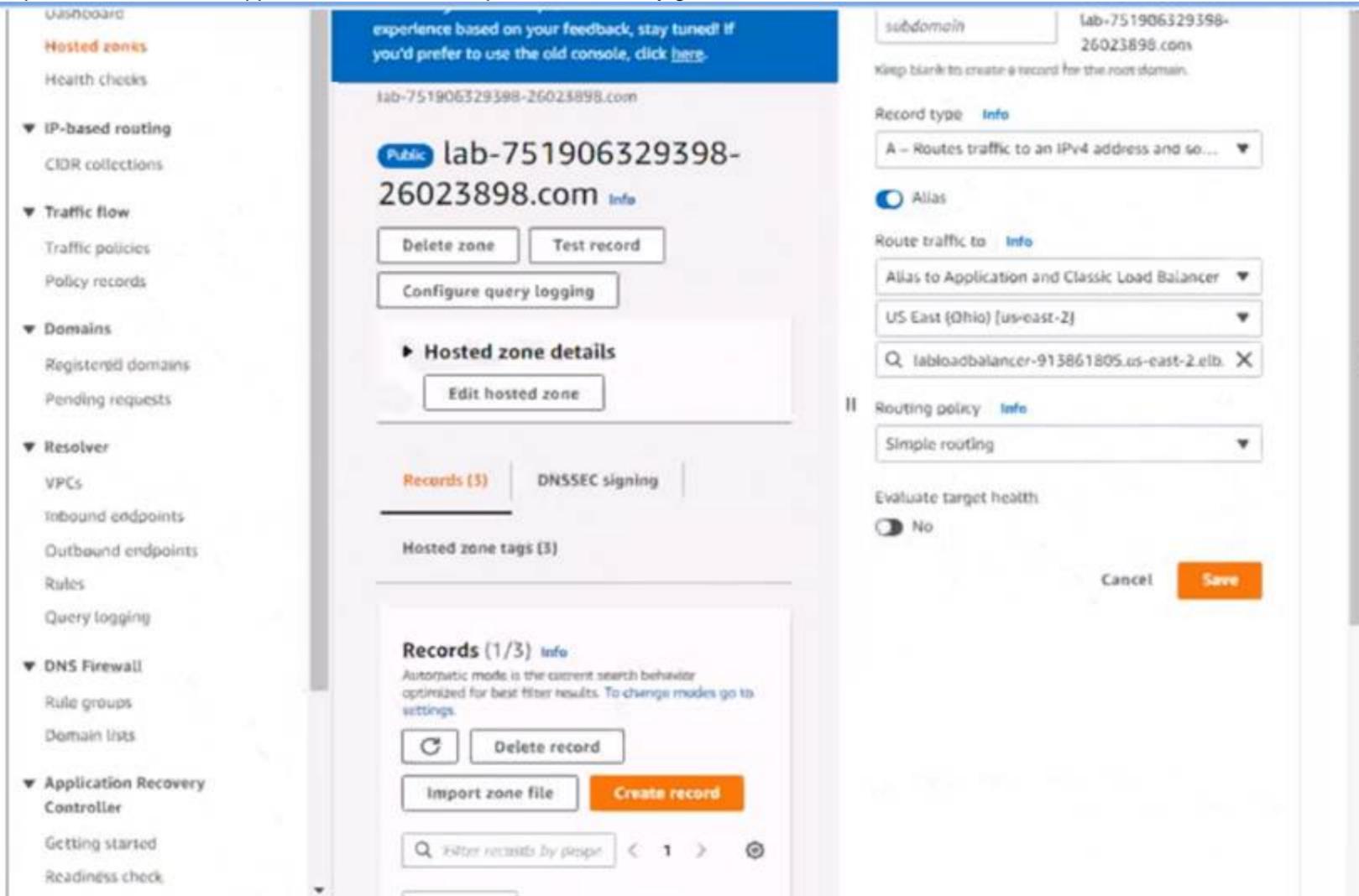
This could be because you don't have permissions to access AWS Health. Please contact your account administrator.



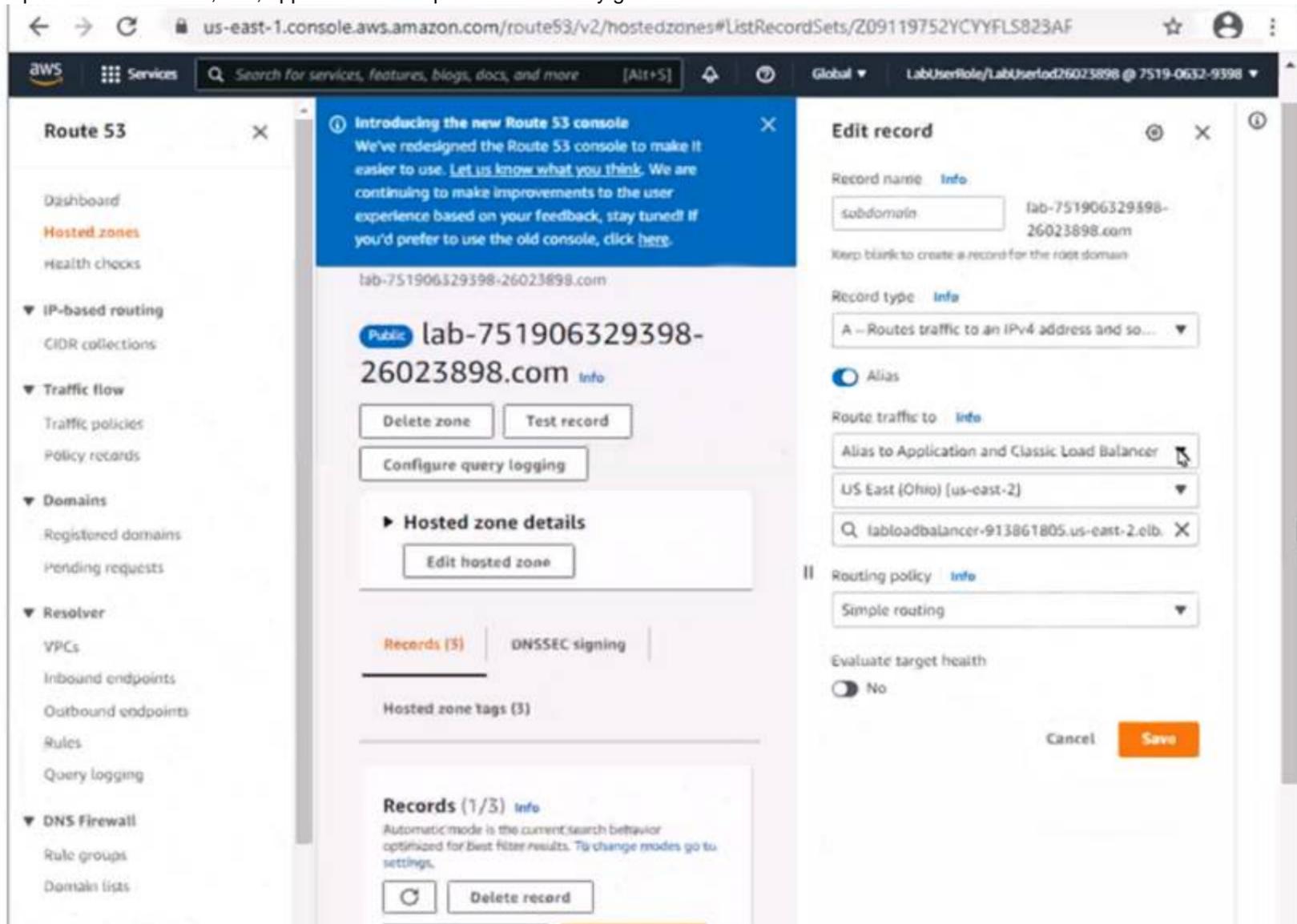
Graphical user interface, text, application Description automatically generated

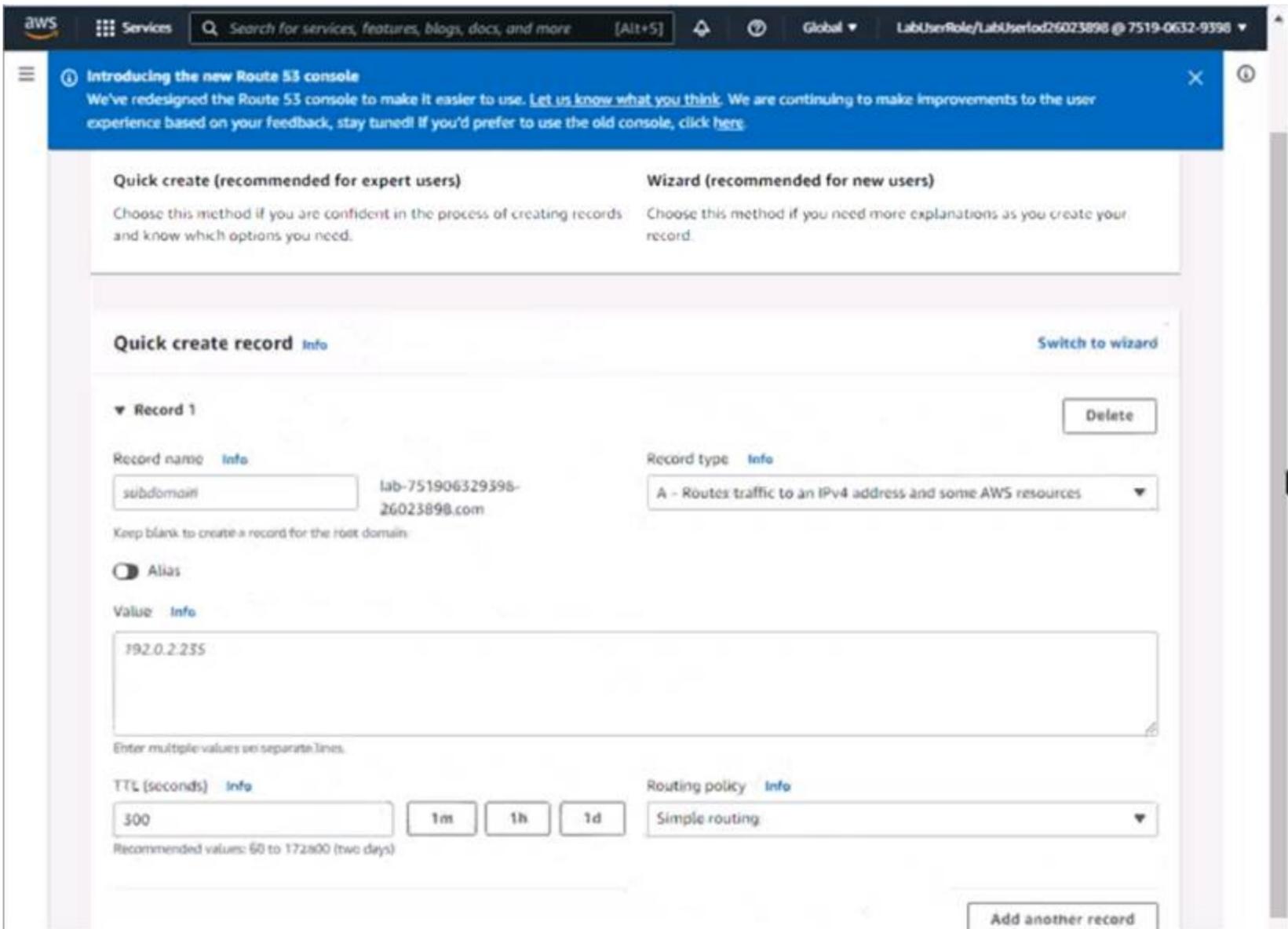


Graphical user interface, application, Teams Description automatically generated

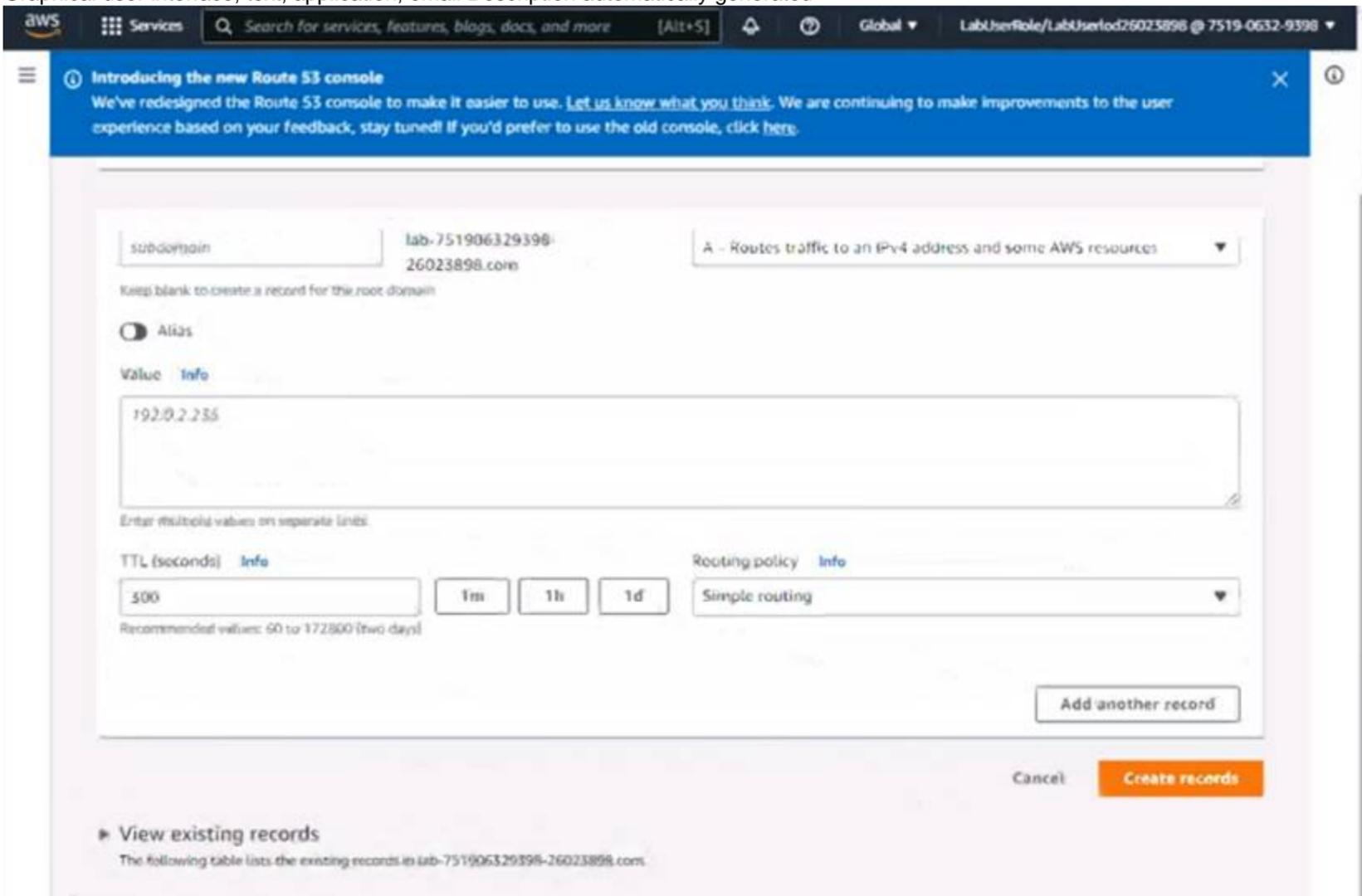


Graphical user interface, text, application Description automatically generated





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

Keep blank to create a record for the root domain.

Record type Info

Alias

Route traffic to Info

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: Z09119752YCYF5823AF

Routing policy Info

Failover record type

Health check ID - optional Info

Evaluate target health

 Yes

Record ID Info

Add another record

We've redesigned the console to continue to make it easier to use and 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

Keep blank to create a record for the root domain.

Record type Info

Alias

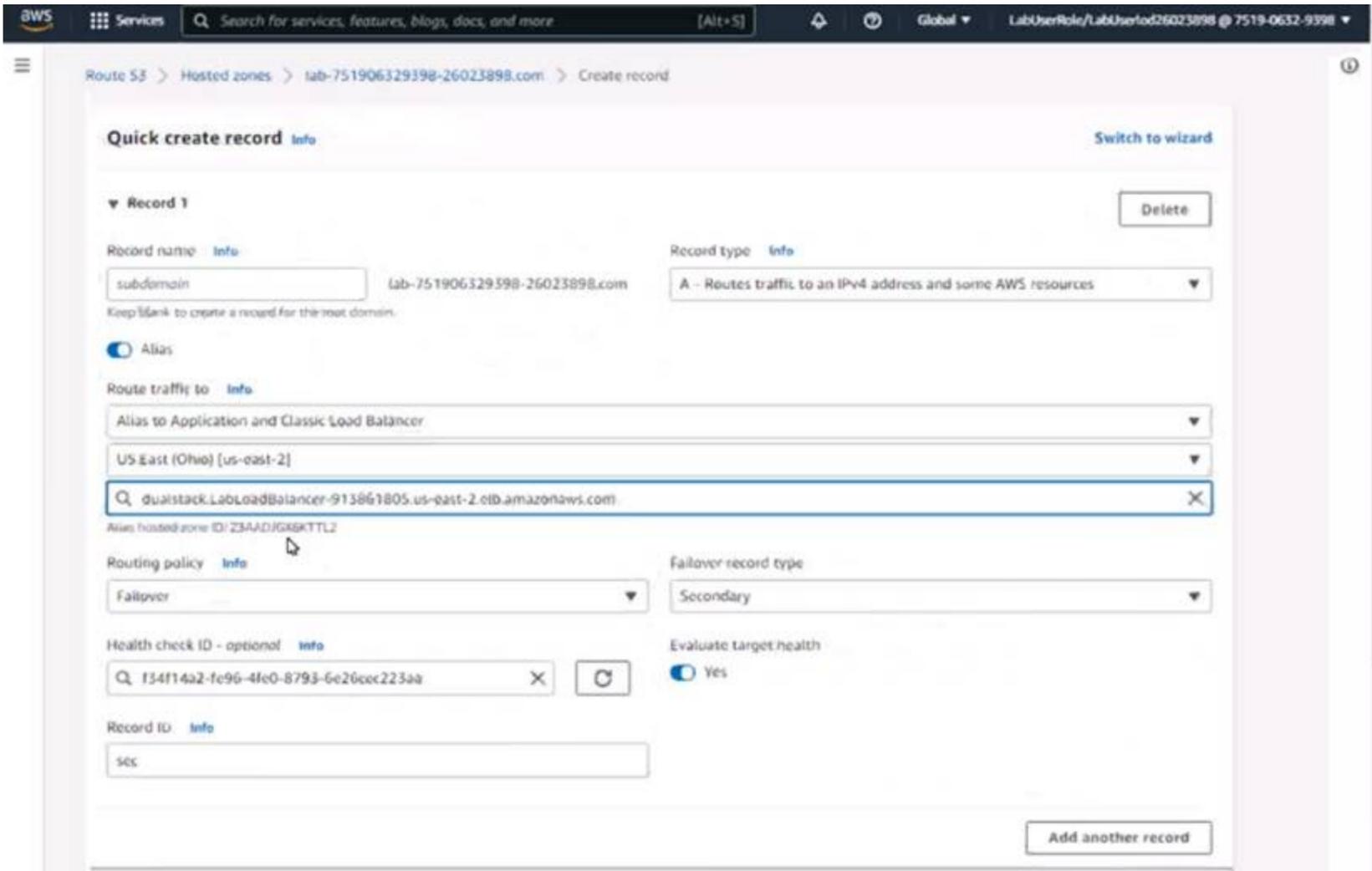
Route traffic to Info

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: Z09119752YCYF5823AF

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 344

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual AWS-Certified-SysOps-Administrator-Associate Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the AWS-Certified-SysOps-Administrator-Associate Product From:

<https://www.2passeasy.com/dumps/AWS-Certified-SysOps-Administrator-Associate/>

Money Back Guarantee

AWS-Certified-SysOps-Administrator-Associate Practice Exam Features:

- * AWS-Certified-SysOps-Administrator-Associate Questions and Answers Updated Frequently
- * AWS-Certified-SysOps-Administrator-Associate Practice Questions Verified by Expert Senior Certified Staff
- * AWS-Certified-SysOps-Administrator-Associate Most Realistic Questions that Guarantee you a Pass on Your First Try
- * AWS-Certified-SysOps-Administrator-Associate Practice Test Questions in Multiple Choice Formats and Updates for 1 Year