

Amazon-Web-Services

Exam Questions SOA-C02

AWS Certified SysOps Administrator - Associate (SOA-C02)



NEW QUESTION 1

- (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 2

- (Exam Topic 1)

A SysOps administrator receives an alert from Amazon GuardDuty about suspicious network activity on an Amazon EC2 instance. The GuardDuty finding lists a new external IP address as a traffic destination. The SysOps administrator does not recognize the external IP address. The SysOps administrator must block traffic to the external IP address that GuardDuty identified.

Which solution will meet this requirement?

- A. Create a new security group to block traffic to the external IP address.
- B. Assign the new security group to the EC2 instance.
- C. Use VPC flow logs with Amazon Athena to block traffic to the external IP address.
- D. Create a network ACL.
- E. Add an outbound deny rule for traffic to the external IP address.
- F. Create a new security group to block traffic to the external IP address.
- G. Assign the new security group to the entire VPC.

Answer: C

Explanation:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html>

NEW QUESTION 3

- (Exam Topic 1)

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

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

Answer: A

Explanation:

Using Amazon S3 Block Public Access

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

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

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

NEW QUESTION 4

- (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

Explanation:

The best combination of steps to meet this requirement is to sign in to the new account by using root user credentials and change the support plan, and to create an IAM user that has administrator privileges in the new account.

Signing in to the new account by using root user credentials will allow the SysOps administrator to access the account and change the support plan to AWS Business Support. Additionally, creating an IAM user that has administrator privileges in the new account will ensure that the SysOps administrator has the necessary access to manage the account and make changes to the support plan if necessary.

Reference:

[1] https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_access.html#orgs_ma

NEW QUESTION 5

- (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 6

- (Exam Topic 1)

A SysOps administrator must set up notifications for whenever combined billing exceeds a certain threshold for all AWS accounts within a company. The administrator has set up AWS Organizations and enabled Consolidated Billing.

Which additional steps must the administrator perform to set up the billing alerts?

- A. In the payer account: Enable billing alerts in the Billing and Cost Management console; publish an Amazon SNS message when the billing alert triggers.
- B. In each account: Enable billing alerts in the Billing and Cost Management console; set up a billing alarm in Amazon CloudWatch; publish an SNS message when the alarm triggers.
- C. In the payer account: Enable billing alerts in the Billing and Cost Management console; set up a billing alarm in the Billing and Cost Management console to publish an SNS message when the alarm triggers.
- D. In the payer account: Enable billing alerts in the Billing and Cost Management console; set up a billing alarm in Amazon CloudWatch; publish an SNS message when the alarm triggers.

Answer: D

NEW QUESTION 7

- (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 8

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

Answer: B

NEW QUESTION 9

- (Exam Topic 1)

A SysOps administrator receives an alert from Amazon GuardDuty about suspicious network activity on an Amazon EC2 instance. The GuardDuty finding lists a new external IP address as a traffic destination. The SysOps administrator does not recognize the external IP address. The SysOps administrator must block traffic to the external IP address that GuardDuty identified.

Which solution will meet this requirement?

- A. Create a new security group to block traffic to the external IP address.
- B. Assign the new security group to the EC2 instance.
- C. Use VPC flow logs with Amazon Athena to block traffic to the external IP address.
- D. Create a network ACL. Add an outbound deny rule for traffic to the external IP address.
- E. Create a new security group to block traffic to the external IP address. Assign the new security group to the entire VPC.

Answer: A

NEW QUESTION 10

- (Exam Topic 1)

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

Which AWS feature should the SysOps administrator use to meet these requirements?

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

Answer: C

NEW QUESTION 10

- (Exam Topic 1)

A SysOps administrator needs to develop a solution that provides email notification and inserts a record into a database every time a file is put into an Amazon S3 bucket.

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

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

Answer: C

NEW QUESTION 15

- (Exam Topic 1)

A company has two VPC networks named VPC A and VPC B. The VPC A CIDR block is 10.0.0.0/16 and the VPC B CIDR block is 172.31.0.0/16. The company wants to establish a VPC peering connection named pcx-12345 between both VPCs.

Which rules should appear in the route table of VPC A after configuration? (Select TWO.)

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

Answer: AD

Explanation:

<https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-routing.html>

NEW QUESTION 20

- (Exam Topic 1)

A SysOps administrator needs to create alerts that are based on the read and write metrics of Amazon Elastic Block Store (Amazon EBS) volumes that are attached to an Amazon EC2 instance. The SysOps administrator creates and enables Amazon CloudWatch alarms for the DiskReadBytes metric and the DiskWriteBytes metric.

A custom monitoring tool that is installed on the EC2 instance with the same alarm configuration indicates that the volume metrics have exceeded the threshold. However, the CloudWatch alarms were not in ALARM state.

Which action will ensure that the CloudWatch alarms function correctly?

- A. Install and configure the CloudWatch agent on the EC2 instance to capture the desired metrics.
- B. Install and configure AWS Systems Manager Agent on the EC2 instance to capture the desired metrics.
- C. Reconfigure the CloudWatch alarms to use the VolumeReadBytes metric and the VolumeWriteBytes metric for the EBS volumes.
- D. Reconfigure the CloudWatch alarms to use the VolumeReadBytes metric and the VolumeWriteBytes metric for the EC2 instance.

Answer: A

NEW QUESTION 22

- (Exam Topic 1)

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

Which backup solution will meet these requirements?

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

Answer: D

Explanation:

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

NEW QUESTION 26

- (Exam Topic 1)

A company uses AWS Organizations to manage multiple AWS accounts with consolidated billing enabled. Organization member account owners want the benefits of Reserved Instances (RIs) but do not want to share RIs with other accounts.

Which solution will meet these requirements?

- A. Purchase RIs in individual member account.
- B. Disable RI discount sharing in the management account.
- C. Purchase RIs in individual member account.
- D. Disable RI discount sharing in the member accounts.
- E. Purchase RIs in the management account.
- F. Disable RI discount sharing in the management account.
- G. Purchase RIs in the management account.
- H. Disable RI discount sharing in the member accounts.

Answer: A

Explanation:

<https://aws.amazon.com/premiumsupport/knowledge-center/ec2-ri-consolidated-billing/>

RI discounts apply to accounts in an organization's consolidated billing family depending upon whether RI sharing is turned on or off for the accounts. By default, RI sharing for all accounts in an organization is turned on. The management account of an organization can change this setting by turning off RI sharing for an account. The capacity reservation for an RI applies only to the account the RI was purchased on, no matter whether RI sharing is turned on or off.

NEW QUESTION 31

- (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 35

- (Exam Topic 1)

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

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

What is one cause of the problem?

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

Answer: D

NEW QUESTION 40

- (Exam Topic 1)

A development team recently deployed a new version of a web application to production. After the release, penetration testing revealed a cross-site scripting vulnerability that could expose user data. Which AWS service will mitigate this issue?

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

Answer: B

Explanation:

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

NEW QUESTION 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 46

- (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 48

- (Exam Topic 1)

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

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

Answer: B

Explanation:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-dependson.html> Syntax The DependsOn attribute can take a single string or list of strings. "DependsOn" : [String, ...]

Example The following template contains an AWS::EC2::Instance resource with a DependsOn attribute that specifies myDB, an AWS::RDS::DBInstance. When CloudFormation creates this stack, it first creates myDB, then creates Ec2Instance.

NEW QUESTION 53

- (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 55

- (Exam Topic 1)

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

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

Answer: AC

NEW QUESTION 59

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 60

- (Exam Topic 1)

A company's reporting job that used to run in 15 minutes is now taking an hour to run. An application generates the reports. The application runs on Amazon EC2 instances and extracts data from an Amazon RDS for MySQL database. A SysOps administrator checks the Amazon CloudWatch dashboard for the RDS instance and notices that the Read IOPS metrics are high, even when the reports are not running. The SysOps administrator needs to improve the performance and the availability of the RDS instance. Which solution will meet these requirements?

- A. Configure an Amazon ElastiCache cluster in front of the RDS instance.
- B. Update the reporting job to query the ElastiCache cluster.
- C. Deploy an RDS read replica.
- D. Update the reporting job to query the reader endpoint.
- E. Create an Amazon CloudFront distribution.
- F. Set the RDS instance as the origin.
- G. Update the reporting job to query the CloudFront distribution.
- H. Increase the size of the RDS instance.

Answer: B

Explanation:

Using an RDS read replica will improve the performance and availability of the RDS instance by offloading read queries to the replica. This will also ensure that the reporting job completes in a timely manner and does not affect the performance of other queries that might be running on the RDS instance. Additionally, updating the reporting job to query the reader endpoint will ensure that all read queries are directed to the read replica.

Reference: [1] https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

NEW QUESTION 61

- (Exam Topic 1)

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

- A. Associate a secondary IPv4 CIDR block with the VPC.
- B. Associate a primary IPv6 CIDR block with the VPC.
- C. Create a new subnet for the VPC.
- D. Modify the CIDR block of the VPC.
- E. Modify the CIDR block of the subnet that is associated with the instances.

Answer: AD

NEW QUESTION 63

- (Exam Topic 1)

A SysOps administrator is testing an application that is hosted on five Amazon EC2 instances. The instances run in an Auto Scaling group behind an Application

Load Balancer (ALB) High CPU utilization during load testing is causing the Auto Scaling group to scale out. The SysOps administrator must troubleshoot to find the root cause of the high CPU utilization before the Auto Scaling group scales out. Which action should the SysOps administrator take to meet these requirements?

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

Answer: A

NEW QUESTION 66

- (Exam Topic 1)

A company has a stateless application that is hosted on a fleet of 10 Amazon EC2 On-Demand Instances in an Auto Scaling group. A minimum of 6 instances are needed to meet service requirements.

Which action will maintain uptime for the application MOST cost-effectively?

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

Answer: A

NEW QUESTION 71

- (Exam Topic 1)

A SysOps administrator is troubleshooting an AWS CloudFormation template whereby multiple Amazon EC2 instances are being created. The template is working in us-east-1, but it is failing in us-west-2 with the error code:

```
AMI [ami-12345678] does not exist
```

How should the administrator ensure that the AWS CloudFormation template is working in every region?

- A. Copy the source region's Amazon Machine Image (AMI) to the destination region and assign it the same ID.
- B. Edit the AWS CloudFormation template to specify the region code as part of the fully qualified AMI ID.
- C. Edit the AWS CloudFormation template to offer a drop-down list of all AMIs to the user by using the `aws::EC2::ami::imageId` control.
- D. Modify the AWS CloudFormation template by including the AMI IDs in the "Mappings" section.
- E. Refer to the proper mapping within the template for the proper AMI ID.

Answer: A

NEW QUESTION 73

- (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: A

Explanation:

<https://aws.amazon.com/blogs/security/control-access-to-aws-resources-by-using-the-aws-organization-of-iam-p>

NEW QUESTION 74

- (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 76

- (Exam Topic 1)

A SysOps administrator is creating an Amazon EC2 Auto Scaling group in a new AWS account. After adding some instances, the SysOps administrator notices that the group has not reached the minimum number of instances. The SysOps administrator receives the following error message:

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

Which action will resolve this issue?

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

Answer: C

NEW QUESTION 79

- (Exam Topic 1)

A company creates custom AMI images by launching new Amazon EC2 instances from an AWS CloudFormation template it installs and configure necessary software through AWS OpsWorks and takes images of each EC2 instance. The process of installing and configuring software can take between 2 to 3 hours but at times the process stalls due to installation errors.

The SysOps administrator must modify the CloudFormation template so if the process stalls, the entire stack will tail and roil back.

Based on these requirements what should be added to the template?

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

Answer: B

NEW QUESTION 82

- (Exam Topic 1)

A SysOps administrator receives notification that an application that is running on Amazon EC2 instances has failed to authenticate to an Amazon RDS database. To troubleshoot, the SysOps administrator needs to investigate AWS Secrets Manager password rotation.

Which Amazon CloudWatch log will provide insight into the password rotation?

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

Answer: B

NEW QUESTION 87

- (Exam Topic 1)

A company has an Amazon RDS DB instance. The company wants to implement a caching service while maintaining high availability.

Which combination of actions will meet these requirements? (Choose two.)

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

Answer: CD

Explanation:

<https://aws.amazon.com/elasticache/memcached/> <https://aws.amazon.com/elasticache/redis/>

NEW QUESTION 88

- (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 volum
- E. Replace the original volume with a volume that is created from the snapshot.

Answer: B

NEW QUESTION 89

- (Exam Topic 1)

A company uses AWS Organizations to manage multiple AWS accounts. The company's SysOps team has been using a manual process to create and manage

1AM roles. The team requires an automated solution to create and manage the necessary 1AM roles for multiple AWS accounts. What is the MOST operationally efficient solution that meets these requirements?

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

Answer: D

NEW QUESTION 93

- (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 98

- (Exam Topic 1)

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

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

Answer: AC

Explanation:

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

NEW QUESTION 99

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 103

- (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 107

- (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 tiles, but the object names remained the same. Users report that old content is still appearing on the website.

How should a SysOps administrator remediate this issue?

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

Answer: A

NEW QUESTION 108

- (Exam Topic 1)

A company is using an Amazon DynamoDB table for data. A SysOps administrator must configure replication of the table to another AWS Region for disaster recovery.

What should the SysOps administrator do to meet this requirement?

- A. Enable DynamoDB Accelerator (DAX).
- B. Enable DynamoDB Streams, and add a global secondary index (GSI).
- C. Enable DynamoDB Streams, and-add a global table Region.
- D. Enable point-in-time recovery.

Answer: C

NEW QUESTION 113

- (Exam Topic 1)

A company's IT department noticed an increase in the spend of their developer AWS account. There are over 50 developers using the account, and the finance team wants to determine the service costs incurred by each developer.

What should a SysOps administrator do to collect this information? (Select TWO.)

- A. Activate the createdBy tag in the account.
- B. Analyze the usage with Amazon CloudWatch dashboards.
- C. Analyze the usage with Cost Explorer.
- D. Configure AWS Trusted Advisor to track resource usage.
- E. Create a billing alarm in AWS Budgets.

Answer: AC

NEW QUESTION 114

- (Exam Topic 1)

A SysOps administrator must configure a resilient tier of Amazon EC2 instances for a high performance computing (HPC) application. The HPC application requires minimum latency between nodes

Which actions should the SysOps administrator take to meet these requirements? (Select TWO.)

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

Answer: AD

NEW QUESTION 116

- (Exam Topic 1)

A SysOps administrator is building a process for sharing Amazon RDS database snapshots between different accounts associated with different business units within the same company. All data must be encrypted at rest.

How should the administrator implement this process?

- A. Write a script to download the encrypted snapshot, decrypt it using the AWS KMS encryption key used to encrypt the snapshot, then create a new volume in each account.
- B. Update the key policy to grant permission to the AWS KMS encryption key used to encrypt the snapshot with all relevant accounts, then share the snapshot with those accounts.
- C. Create an Amazon EC2 instance based on the snapshot, then save the instance's Amazon EBS volume as a snapshot and share it with the other account
- D. Require each account owner to create a new volume from that snapshot and encrypt it.
- E. Create a new unencrypted RDS instance from the encrypted snapshot, connect to the instance using SSH/RD
- F. export the database contents into a file, then share this file with the other accounts.

Answer: B

NEW QUESTION 121

- (Exam Topic 1)

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

What should the SysOps administrator do to meet these requirements?

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

Answer: C

Explanation:

You might want to use Transfer Acceleration on a bucket for various reasons: ->Your customers upload to a centralized bucket from all over the world. ->You transfer gigabytes to terabytes of data on a regular basis across continents. ->You can't use all of your available bandwidth over the internet when uploading to Amazon S3." <https://docs.aws.amazon.com/AmazonS3/latest/userguide/transfer-acceleration.html>

NEW QUESTION 124

- (Exam Topic 1)

A company hosts a database on an Amazon RDS Multi-AZ DB instance. The database is not encrypted. The company's new security policy requires all AWS resources to be encrypted at rest and in transit.

What should a SysOps administrator do to encrypt the database?

- A. Configure encryption on the existing DB instance.
- B. Take a snapshot of the DB instance.
- C. Encrypt the snapshot.
- D. Restore the snapshot to the same DB instance.
- E. Encrypt the standby replica in a secondary Availability Zone.
- F. Promote the standby replica to the primary DB instance.
- G. Take a snapshot of the DB instance.
- H. Copy and encrypt the snapshot.
- I. Create a new DB instance by restoring the encrypted copy.

Answer: B

NEW QUESTION 125

- (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 a CNAME 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 129

- (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 133

- (Exam Topic 1)

A company is trying to connect two applications. One application runs in an on-premises data center that has a hostname of host1.onprem.private. The other

application runs on an Amazon EC2 instance that has a hostname of `hostl.awscloud.private`. An AWS Site-to-Site VPN connection is in place between the on-premises network and AWS.

The application that runs in the data center tries to connect to the application that runs on the EC2 instance, but DNS resolution fails. A SysOps administrator must implement DNS resolution between on-premises and AWS resources.

Which solution allows the on-premises application to resolve the EC2 instance hostname?

- A. Set up an Amazon Route 53 inbound resolver endpoint with a forwarding rule for the `onprem.private` hosted zone
- B. Associate the resolver with the VPC of the EC2 instance
- C. Configure the on-premises DNS resolver to forward `onprem.private` DNS queries to the inbound resolver endpoint.
- D. Set up an Amazon Route 53 inbound resolver endpoint
- E. Associate the resolver with the VPC of the EC2 instance
- F. Configure the on-premises DNS resolver to forward `awscloud.private` DNS queries to the inbound resolver endpoint.
- G. Set up an Amazon Route 53 outbound resolver endpoint with a forwarding rule for the `onprem.private` hosted zone
- H. Associate the resolver with the AWS Region of the EC2 instance
- I. Configure the on-premises DNS resolver to forward `onprem.private` DNS queries to the outbound resolver endpoint.
- J. Set up an Amazon Route 53 outbound resolver endpoint
- K. Associate the resolver with the AWS Region of the EC2 instance
- L. Configure the on-premises DNS resolver to forward `awscloud.private` DNS queries to the outbound resolver endpoint.

Answer: C

NEW QUESTION 136

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 140

- (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 143

- (Exam Topic 1)

A company's SysOps administrator needs to change the AWS Support plan for one of the company's AWS accounts. The account has multi-factor authentication (MFA) activated, and the MFA device is lost.

What should the SysOps administrator do to sign in?

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

Answer: A

NEW QUESTION 144

- (Exam Topic 1)

A company hosts an internal application on Amazon EC2 instances. All application data and requests route through an AWS Site-to-Site VPN connection between the on-premises network and AWS. The company must monitor the application for changes that allow network access outside of the corporate network. Any change that exposes the application externally must be restricted automatically.

Which solution meets these requirements in the MOST operationally efficient manner?

- A. Create an AWS Lambda function that updates security groups that are associated with the elastic network interface to remove inbound rules with noncorporate CIDR range.

- B. Turn on VPC Flow Logs, and send the logs to Amazon CloudWatch Log
- C. Create an Amazon CloudWatch alarm that matches traffic from noncorporate CIDR ranges, and publish a message to an Amazon Simple Notification Service (Amazon SNS) topic with the Lambda function as a target.
- D. Create a scheduled Amazon EventBridge (Amazon CloudWatch Events) rule that targets an AWS Systems Manager Automation document to check for public IP addresses on the EC2 instance
- E. If public IP addresses are found on the EC2 instances, initiate another Systems Manager Automation document to terminate the instances.
- F. Configure AWS Config and a custom rule to monitor whether a security group allows inbound requests from noncorporate CIDR range
- G. Create an AWS Systems Manager Automation document to remove any noncorporate CIDR ranges from the application security groups.
- H. Configure AWS Config and the managed rule for monitoring public IP associations with the EC2 instances by ta
- I. Tag the EC2 instances with an identify
- J. Create an AWS Systems Manager Automation document to remove the public IP association from the EC2 instances.

Answer: C

Explanation:

<https://aws.amazon.com/blogs/security/how-to-auto-remediate-internet-accessible-ports-with-aws-config-and-aws-lambda/>

NEW QUESTION 149

- (Exam Topic 1)

A company is implementing a monitoring solution that is based on machine learning. The monitoring solution consumes Amazon EventBridge (Amazon CloudWatch Events) events that are generated by Amazon EC2 Auto Scaling. The monitoring solution provides detection of anomalous behavior such as unanticipated scaling events and is configured as an EventBridge (CloudWatch Events) API destination. During initial testing, the company discovers that the monitoring solution is not receiving events. However, Amazon CloudWatch is showing that the EventBridge (CloudWatch Events) rule is being invoked. A SysOps administrator must implement a solution to retrieve client error details to help resolve this issue. Which solution will meet these requirements with the LEAST operational effort?

- A. Create an EventBridge (CloudWatch Events) archive for the event pattern to replay the event
- B. Increase the logging on the monitoring solution
- C. Use replay to invoke the monitoring solution
- D. Examine the error details.
- E. Add an Amazon Simple Queue Service (Amazon SQS) standard queue as a dead-letter queue for the target
- F. Process the messages in the dead-letter queue to retrieve error details.
- G. Create a second EventBridge (CloudWatch Events) rule for the same event pattern to target an AWS Lambda function
- H. Configure the Lambda function to invoke the monitoring solution and to record the results to Amazon CloudWatch Log
- I. Examine the errors in the logs.
- J. Configure the EventBridge (CloudWatch Events) rule to send error messages to an Amazon Simple Notification Service (Amazon SNS) topic.

Answer: A

Explanation:

"In EventBridge, you can create an archive of events so that you can easily replay them at a later time. For example, you might want to replay events to recover from errors or to validate new functionality in your application." <https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-archive.html>

NEW QUESTION 150

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 155

- (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 160

- (Exam Topic 1)

A company uses AWS CloudFormation templates to deploy cloud infrastructure. An analysis of all the company's templates shows that the company has declared the same components in multiple templates. A SysOps administrator needs to create dedicated templates that have their own parameters and conditions for these common components. Which solution will meet this requirement?

- A. Develop a CloudFormation change set.

- B. Develop CloudFormation macros.
- C. Develop CloudFormation nested stacks.
- D. Develop CloudFormation stack sets.

Answer: C

NEW QUESTION 164

- (Exam Topic 1)

A company has a simple web application that runs on a set of Amazon EC2 instances behind an Elastic Load Balancer in the eu-west-2 Region. Amazon Route 53 holds a DNS record for the application with a simple routing policy. Users from all over the world access the application through their web browsers.

The company needs to create additional copies of the application in the us-east-1 Region and in the ap-south-1 Region. The company must direct users to the Region that provides the fastest response times when the users load the application.

What should a SysOps administrator do to meet these requirements?

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

Answer: B

NEW QUESTION 167

- (Exam Topic 1)

A company stores sensitive data in an Amazon S3 bucket. The company must log all access attempts to the S3 bucket. The company's risk team must receive immediate notification about any delete events.

Which solution will meet these requirements?

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

Answer: A

Explanation:

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

NEW QUESTION 168

- (Exam Topic 1)

A company is storing backups in an Amazon S3 bucket. The backups must not be deleted for at least 3 months after the backups are created.

What should a SysOps administrator do to meet this requirement?

- A. Configure an IAM policy that denies the s3:DeleteObject action for all user
- B. Three months after an object is written, remove the policy.
- C. Enable S3 Object Lock on a new S3 bucket in compliance mode
- D. Place all backups in the new S3 bucket with a retention period of 3 months.
- E. Enable S3 Versioning on the existing S3 bucket
- F. Configure S3 Lifecycle rules to protect the backups.
- G. Enable S3 Object Lock on a new S3 bucket in governance mode
- H. Place all backups in the new S3 bucket with a retention period of 3 months.

Answer: D

Explanation:

To meet the requirements of the workload, a SysOps administrator should enable S3 Object Lock on a new S3 bucket in governance mode and place all backups in the new S3 bucket with a retention period of 3 months.

This will ensure that the backups are not deleted for at least 3 months after they are created. The other solutions (configuring an IAM policy that denies the s3:DeleteObject action for all users, enabling S3 Object Lock on a new S3 bucket in compliance mode, or enabling S3 Versioning on the existing S3 bucket and configuring S3 Lifecycle rules to protect the backups) will not meet the requirements, as they do not provide a way to ensure that the backups are not deleted for at least 3 months after they are created.

NEW QUESTION 169

- (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 171

- (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 173

- (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 176

- (Exam Topic 1)

A company recently purchased Savings Plans. The company wants to receive email notification when the company's utilization drops below 90% for a given day. Which solution will meet this requirement?

- A. Create an Amazon CloudWatch alarm to monitor the Savings Plan check in AWS Trusted Advisor. Configure an Amazon Simple Queue Service (Amazon SQS) queue for email notification when the utilization drops below 90% for a given day.
- B. Create an Amazon CloudWatch alarm to monitor the SavingsPlansUtilization metric under the AWS/SavingsPlans namespace in CloudWatch
- C. Configure an Amazon Simple Queue Service (Amazon SQS) queue for email notification when the utilization drops below 90% for a given day.
- D. Create a Savings Plans alert to monitor the daily utilization of the Savings Plan
- E. Configure an Amazon Simple Notification Service (Amazon SNS) topic for email notification when the utilization drops below 90% for a given day.
- F. Use AWS Budgets to create a Savings Plans budget to track the daily utilization of the Savings Plans. Configure an Amazon Simple Notification Service (Amazon SNS) topic for email notification when the utilization drops below 90% for a given day.

Answer: D

Explanation:

AWS Budgets can be used to create a Savings Plans budget and track the daily utilization of the company's Savings Plans. By creating a budget, it will trigger an action when the utilization drops below 90%, which in this case will be to send an email notification via an Amazon SNS topic. This will ensure that the company is notified when their Savings Plans utilization drops below 90%, allowing them to take action if necessary.

Reference: [1] <https://docs.aws.amazon.com/savingsplans/latest/userguide/sp-usingBudgets.html>

NEW QUESTION 179

- (Exam Topic 1)

A company uses an Amazon CloudFront distribution to deliver its website. Traffic logs for the website must be centrally stored, and all data must be encrypted at rest.

Which solution will meet these requirements?

- A. Create an Amazon OpenSearch Service (Amazon Elasticsearch Service) domain with internet access and server-side encryption that uses the default AWS managed key
- B. Configure CloudFront to use the Amazon OpenSearch Service (Amazon Elasticsearch Service) domain as a log destination.
- C. Create an Amazon OpenSearch Service (Amazon Elasticsearch Service) domain with VPC access and server-side encryption that uses AES-256. Configure CloudFront to use the Amazon OpenSearch Service (Amazon Elasticsearch Service) domain as a log destination.
- D. Create an Amazon S3 bucket that is configured with default server-side encryption that uses AES-256. Configure CloudFront to use the S3 bucket as a log destination.

- E. Create an Amazon S3 bucket that is configured with no default encryption
- F. Enable encryption in the CloudFront distribution, and use the S3 bucket as a log destination.

Answer: C

NEW QUESTION 181

- (Exam Topic 1)

A SysOps administrator is configuring an application on Amazon EC2 instances for a company Teams in other countries will use the application over the internet. The company requires the application endpoint to have a static public IP address. How should the SysOps administrator deploy the application to meet this requirement?

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

Answer: C

NEW QUESTION 183

- (Exam Topic 1)

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

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

Answer: D

Explanation:

Automated way to update your image. Have a pipeline to update your image. When you boot from your AMI, updates = scripts are already pre-installed, so no need to complete boot scripts in boot process. <https://aws.amazon.com/image-builder/>

NEW QUESTION 185

- (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 188

- (Exam Topic 1)

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

- A. Create an Amazon OpenSearch Service (Amazon Elasticsearch Service) domain with internet access and server-side encryption that uses the default AWS managed key. Configure CloudFront to use the Amazon OpenSearch Service (Amazon Elasticsearch Service) domain as a log destination.
- B. Create an Amazon OpenSearch Service (Amazon Elasticsearch Service) domain with VPC access and server-side encryption that uses AES-256. Configure CloudFront to use the Amazon OpenSearch Service (Amazon Elasticsearch Service) domain as a log destination.

- C. Create an Amazon S3 bucket that is configured with default server side encryption that uses AES-256 Configure CloudFront to use the S3 bucket as a log destination
- D. Create an Amazon S3 bucket that is configured with no default encryption Enable encryption in the CloudFront console and use the S3 bucket as a log destination

Answer: C

NEW QUESTION 193

- (Exam Topic 1)

A company is expanding globally and needs to back up data on Amazon Elastic Block Store (Amazon EBS) volumes to a different AWS Region. Most of the EBS volumes that store the data are encrypted, but some of the EBS volumes are unencrypted. The company needs the backup data from all the EBS volumes to be encrypted.

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

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

Answer: A

Explanation:

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

NEW QUESTION 194

- (Exam Topic 1)

A company has an application that runs only on Amazon EC2 Spot Instances. The instances run in an Amazon EC2 Auto Scaling group with scheduled scaling actions.

However, the capacity does not always increase at the scheduled times, and instances terminate many times a day. A Sysops administrator must ensure that the instances launch on time and have fewer interruptions.

Which action will meet these requirements?

- A. Specify the capacity-optimized allocation strategy for Spot Instance
- B. Add more instance types to the Auto Scaling group.
- C. Specify the capacity-optimized allocation strategy for Spot Instance
- D. Increase the size of the instances in the Auto Scaling group.
- E. Specify the lowest-price allocation strategy for Spot Instance
- F. Add more instance types to the Auto Scaling group.
- G. Specify the lowest-price allocation strategy for Spot Instance
- H. Increase the size of the instances in the Auto Scaling group.

Answer: A

Explanation:

Specifying the capacity-optimized allocation strategy for Spot Instances and adding more instance types to the Auto Scaling group is the best action to meet the requirements. Increasing the size of the instances in the Auto Scaling group will not necessarily help with the launch time or reduce interruptions, as the Spot Instances could still be interrupted even with larger instance sizes.

NEW QUESTION 195

- (Exam Topic 1)

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

Which solution will meet these requirements?

- A. Create an AWS Lambda function to call the CreateImage API operation with the EC2 instance ID and the no-reboot parameter enable
- B. Create a daily scheduled Amazon EventBridge (Amazon CloudWatch Events) rule that invokes the function.
- C. Create an AWS Lambda function to call the CreateImage API operation with the EC2 instance ID and the reboot parameter enable
- D. Create a daily scheduled Amazon EventBridge (Amazon CloudWatch Events) rule that invokes the function.
- E. Use AWS Backup to create a backup plan with a backup rule that runs daily
- F. Assign the resource ID of the EC2 instance with the no-reboot parameter enabled.
- G. Use AWS Backup to create a backup plan with a backup rule that runs daily
- H. Assign the resource ID of the EC2 instance with the reboot parameter enabled.

Answer: B

Explanation:

https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/Creating_EBSbacked_WinAMI.html "NoReboot By default, Amazon EC2 attempts to shut down and reboot the instance before creating the image.

If the No Reboot option is set, Amazon EC2 doesn't shut down the instance before creating the image. When this option is used, file system integrity on the created image can't be guaranteed." Besides, we can use AWS EventBridge to invoke Lambda function

https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_CreateImage.html

NEW QUESTION 200

- (Exam Topic 1)

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

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 205

- (Exam Topic 1)

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

Which next step should be taken to configure Route 53?

- A. Create an A record for each serve
- B. Associate the records with the Route 53 HTTP health check.
- C. Create an A record for each serve
- D. Associate the records with the Route 53 TCP health check.
- E. Create an alias record for each server with evaluate target health set to ye
- F. Associate the records with the Route 53 HTTP health check.
- G. Create an alias record for each server with evaluate target health set to ye
- H. Associate the records with the Route 53 TCP health check.

Answer: A

NEW QUESTION 208

- (Exam Topic 1)

A company needs to automatically monitor an AWS account for potential unauthorized AWS Management Console logins from multiple geographic locations.

Which solution will meet this requirement?

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

Answer: D

NEW QUESTION 211

- (Exam Topic 1)

An Amazon EC2 instance needs to be reachable from the internet. The EC2 instance is in a subnet with the following route table:

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

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

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

Answer: C

NEW QUESTION 215

- (Exam Topic 1)

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

To satisfy the requirements, which one of these services can the SysOps administrator enable at-rest encryption on?

- A. EBS General Purpose SSD volumes
- B. RDS PostgreSQL database
- C. Amazon EFS file systems

D. S3 objects within a bucket

Answer: D

Explanation:

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

NEW QUESTION 220

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 221

- (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 224

- (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: A

Explanation:

Glacier Deep Archive retrieval time more than 5 hours (it's 12 hours), so B&D out. S3 Standard IA is cheaper than S3 Standard.

<https://aws.amazon.com/tw/s3/pricing/>

NEW QUESTION 229

- (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 230

- (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 233

- (Exam Topic 1)

A company runs an application on Amazon EC2 instances. The EC2 instances are in an Auto Scaling group and run behind an Application Load Balancer (ALB). The application experiences errors when total requests exceed 100 requests per second. A SysOps administrator must collect information about total requests for a 2-week period to determine when requests exceeded this threshold.

What should the SysOps administrator do to collect this data?

- A. Use the ALB's RequestCount metri
- B. Configure a time range of 2 weeks and a period of 1 minute.Examine the chart to determine peak traffic times and volumes.
- C. Use Amazon CloudWatch metric math to generate a sum of request counts for all the EC2 instances over a 2-week perio
- D. Sort by a 1-minute interval.
- E. Create Amazon CloudWatch custom metrics on the EC2 launch configuration templates to create aggregated request metrics across all the EC2 instances.
- F. Create an Amazon EventBridge (Amazon CloudWatch Events) rul
- G. Configure an EC2 event matching pattern that creates a metric that is based on EC2 request
- H. Display the data in a graph.

Answer: A

Explanation:

Using the ALB's RequestCount metric will allow the SysOps administrator to collect information about total requests for a 2-week period and determine when requests exceeded the threshold of 100 requests per second. Configuring a time range of 2 weeks and a period of 1 minute will ensure that the data can be accurately examined to determine peak traffic times and volumes.

NEW QUESTION 236

- (Exam Topic 1)

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

- A. Deny Pos
- B. Pu
- C. and Delete on the bucket.
- D. Enable server-side encryption on the bucket.
- E. Enable Amazon S3 versioning on the bucket.
- F. Enable snapshots on the bucket.

Answer: B

NEW QUESTION 241

- (Exam Topic 1)

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 246

- (Exam Topic 1)

A SysOps administrator is using AWS Systems Manager Patch Manager to patch a fleet of Amazon EC2 instances. The SysOps administrator has configured a patch baseline and a maintenance window. The SysOps administrator also has used an instance tag to identify which instances to patch.

The SysOps administrator must give Systems Manager the ability to access the EC2 instances. Which additional action must the SysOps administrator perform to meet this requirement?

- A. Add an inbound rule to the instances' security group.
- B. Attach an IAM instance profile with access to Systems Manager to the instances.
- C. Create a Systems Manager activation Then activate the fleet of instances.

D. Manually specify the instances to patch Instead of using tag-based selection.

Answer: A

NEW QUESTION 250

- (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 252

- (Exam Topic 1)

A company using AWS Organizations requires that no Amazon S3 buckets in its production accounts should ever be deleted.

What is the SIMPLEST approach the SysOps administrator can take to ensure S3 buckets in those accounts can never be deleted?

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

Answer: B

Explanation:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html

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

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

NEW QUESTION 253

- (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 255

- (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 257

- (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 identity cost savings.
- B. Create an AWS Budgets alert to alarm when account spend reaches 80% of the budget.
- C. Purchase Reserved Instances through the Amazon EC2 console.
- D. Use AWS Compute Optimizer and take action on the provided recommendations.

Answer: D

NEW QUESTION 262

- (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 266

- (Exam Topic 1)

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

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

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

Answer: C

NEW QUESTION 271

- (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 276

- (Exam Topic 1)

A company is managing many accounts by using a single organization in AWS Organizations. The organization has all features enabled. The company wants to turn on AWS Config in all the accounts of the organization and in all AWS Regions.

What should a SysOps administrator do to meet these requirements in the MOST operationally efficient way?

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

Answer: C

NEW QUESTION 279

- (Exam Topic 1)

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

What must the SysOps administrator do to fix this issue?

- A. Ensure that all the EC2 instances have the correct tags for Systems Manager access.

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

Answer: C

Explanation:

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

NEW QUESTION 283

- (Exam Topic 1)

A company's AWS Lambda function is experiencing performance issues. The Lambda function performs many CPU-intensive operations. The Lambda function is not running fast enough and is creating bottlenecks in the system.

What should a SysOps administrator do to resolve this issue?

- A. In the CPU launch options for the Lambda function, activate hyperthreading.
- B. Turn off the AWS managed encryption.
- C. Increase the amount of memory for the Lambda function.
- D. Load the required code into a custom layer.

Answer: C

Explanation:

Increasing the amount of memory for the Lambda function will help to improve the performance of the function. This is because the Lambda function is CPU-intensive and increasing the memory will give it access to more CPU resources and help it run faster. The other options (activating hyperthreading in the CPU launch options for the Lambda function, turning off the AWS managed encryption, and loading the required code into a custom layer) will not help to improve the performance of the Lambda function and are not the correct solutions for this issue.

<https://docs.aws.amazon.com/lambda/latest/dg/configuration-function-common.html#configuration-memory-con>

NEW QUESTION 284

- (Exam Topic 1)

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

How can this be accomplished?

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

Answer: B

NEW QUESTION 286

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

Answer: B

NEW QUESTION 291

- (Exam Topic 1)

A company has a compliance requirement that no security groups can allow SSH ports to be open to all IP addresses. A SysOps administrator must implement a solution that will notify the company's SysOps team when a security group rule violates this requirement. The solution also must remediate the security group rule automatically.

Which solution will meet these requirements?

- A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function when a security group change
- B. Configure the Lambda function to evaluate the security group for compliance, remove all inbound security group rules on all ports, and notify the SysOps team if the security group is noncompliant.
- C. Create an AWS CloudTrail metric filter for security group change
- D. Create an Amazon CloudWatch alarm to notify the SysOps team through an Amazon Simple Notification Service (Amazon SNS) topic when (he metric is greater than 0. Subscribe an AWS Lambda function to the SNS topic to remediate the security group rule by removing the rule.
- E. Activate the AWS Config restricted-ssh managed rul
- F. Add automatic remediation to the AWS Config rule by using the AWS Systems Manager Automation AWS DisablePublicAccessForSecurityGroup runboo
- G. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to notify the SysOps team when the rule is noncompliant.

- H. Create an AWS CloudTrail metric filter for security group change
- I. Create an Amazon CloudWatch alarm for when the metric is greater than 0. Add an AWS Systems Manager action to the CloudWatch alarm to suspend the security group by using the Systems Manager Automation AWS-DisablePublicAccessForSecurityGroup runbook when the alarm is in ALARM state
- J. Add an Amazon Simple Notification Service (Amazon SNS) topic as a second target to notify the SysOps team.

Answer: C

NEW QUESTION 295

- (Exam Topic 1)

A company migrated an I/O intensive application to an Amazon EC2 general purpose instance. The EC2 instance has a single General Purpose SSD Amazon Elastic Block Store (Amazon EBS) volume attached.

Application users report that certain actions that require intensive reading and writing to the disk are taking much longer than normal or are failing completely. After reviewing the performance metrics of the EBS volume, a SysOps administrator notices that the VolumeQueueLength metric is consistently high during the same times in which the users are reporting issues. The SysOps administrator needs to resolve this problem to restore full performance to the application.

Which action will meet these requirements?

- A. Modify the instance type to be storage optimized.
- B. Modify the volume properties by deselecting Auto-Enable Volume 10.
- C. Modify the volume properties to increase the IOPS.
- D. Modify the instance to enable enhanced networking.

Answer: C

NEW QUESTION 299

- (Exam Topic 1)

A SysOps administrator creates an AWS CloudFormation template to define an application stack that can be deployed in multiple AWS Regions.

The SysOps administrator also creates an Amazon CloudWatch dashboard by using the AWS Management Console. Each deployment of the application requires its own CloudWatch dashboard.

How can the SysOps administrator automate the creation of the CloudWatch dashboard each time the application is deployed?

- A. Create a script by using the AWS CLI to run the aws cloudformation put-dashboard command with the name of the dashboard
- B. Run the command each time a new CloudFormation stack is created.
- C. Export the existing CloudWatch dashboard as JSON
- D. Update the CloudFormation template to define an AWS::CloudWatch::Dashboard resource
- E. Include the exported JSON in the resource's DashboardBody property.
- F. Update the CloudFormation template to define a resource
- G. Use the intrinsic Ref function to reference the ID of the existing CloudWatch dashboard.
- H. Update the CloudFormation template to define an AWS::CloudWatch::Dashboard resource
- I. Specify the name of the existing dashboard in the DashboardName property.

Answer: B

Explanation:

You can only use the Intrinsic Ref function to reference a resource that is being created at the same time as the current CloudFormation template. The question states that the CloudWatch dashboard was previously created using the AWS Management Console, so there is no ID to reference the existing CloudWatch dashboard in the CloudFormation template. You would need to export the existing CloudWatch dashboard as JSON, then use the DashboardBody property in the CloudFormation template to replicate it upon each deployment

(<https://docs.aws.amazon.com/AmazonCloudWatch/latest/APIReference/CloudWatch-Dashboard-Body-Structure.html>)

NEW QUESTION 303

- (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: AD

Explanation:

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

NEW QUESTION 307

- (Exam Topic 1)

A company hosts a website on multiple Amazon EC2 instances that run in an Auto Scaling group. Users are reporting slow responses during peak times between 6 PM and 11 PM every weekend. A SysOps administrator must implement a solution to improve performance during these peak times.

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

- A. Create a scheduled Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function to increase the desired capacity before peak

times.

- B. Configure a scheduled scaling action with a recurrence option to change the desired capacity before and after peak times.
- C. Create a target tracking scaling policy to add more instances when memory utilization is above 70%.
- D. Configure the cooldown period for the Auto Scaling group to modify desired capacity before and after peak times.

Answer: B

Explanation:

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

NEW QUESTION 312

- (Exam Topic 1)

A company hosts an application on an Amazon EC2 instance in a single AWS Region. The application requires support for non-HTTP TCP traffic and HTTP traffic. The company wants to deliver content with low latency by leveraging the AWS network. The company also wants to implement an Auto Scaling group with an Elastic Load Balancer.

How should a SysOps administrator meet these requirements?

- A. Create an Auto Scaling group with an Application Load Balancer (ALB). Add an Amazon CloudFront distribution with the ALB as the origin.
- B. Create an Auto Scaling group with an Application Load Balancer (ALB). Add an accelerator with AWS Global Accelerator with the ALB as an endpoint.
- C. Create an Auto Scaling group with a Network Load Balancer (NLB). Add an Amazon CloudFront distribution with the NLB as the origin.
- D. Create an Auto Scaling group with a Network Load Balancer (NLB). Add an accelerator with AWS Global Accelerator with the NLB as an endpoint.

Answer: D

Explanation:

AWS Global Accelerator and Amazon CloudFront are separate services that use the AWS global network and its edge locations around the world. CloudFront improves performance for both cacheable content (such as images and videos) and dynamic content (such as API acceleration and dynamic site delivery). Global Accelerator improves performance for a wide range of applications over TCP or UDP by proxying packets at the edge to applications running in one or more AWS Regions. Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover. Both services integrate with AWS Shield for DDoS protection.

<https://medium.com/awesome-cloud/aws-difference-between-application-load-balancer-and-network-load-balancer> https://aws.amazon.com/global-accelerator/faqs/?nc1=h_ls

NEW QUESTION 314

- (Exam Topic 2)

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

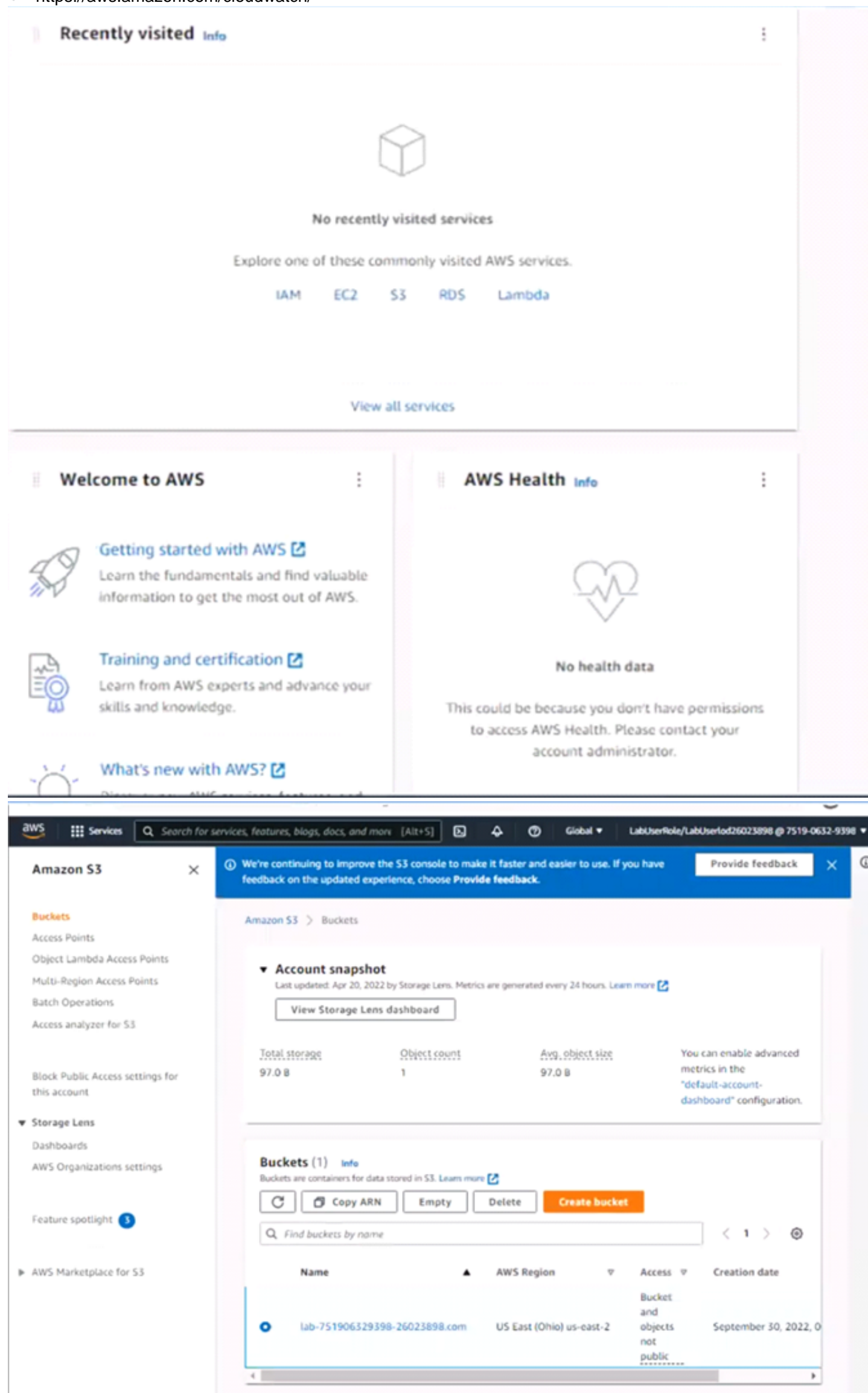
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadGetObject", "Effect": "Allow",
      "Principal": "*", "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::lab-751906329398-26023898.com/*"
    }
  ]
}
```

- Now navigate to the Amazon Route 53 service, and find the existing hosted zone named lab-751906329398-26023898.com.
- Click on the "A record" and update the routing policy to "Primary - Failover" and add the existing ALB as the primary record.
- Click on "Create Record" button and create a new secondary failover alias record for the domain lab-751906329398-26023898.com that routes traffic to the existing S3 bucket.
-

Now, when the primary site (ALB) goes down, traffic will be automatically routed to the S3 bucket serving the static error page.

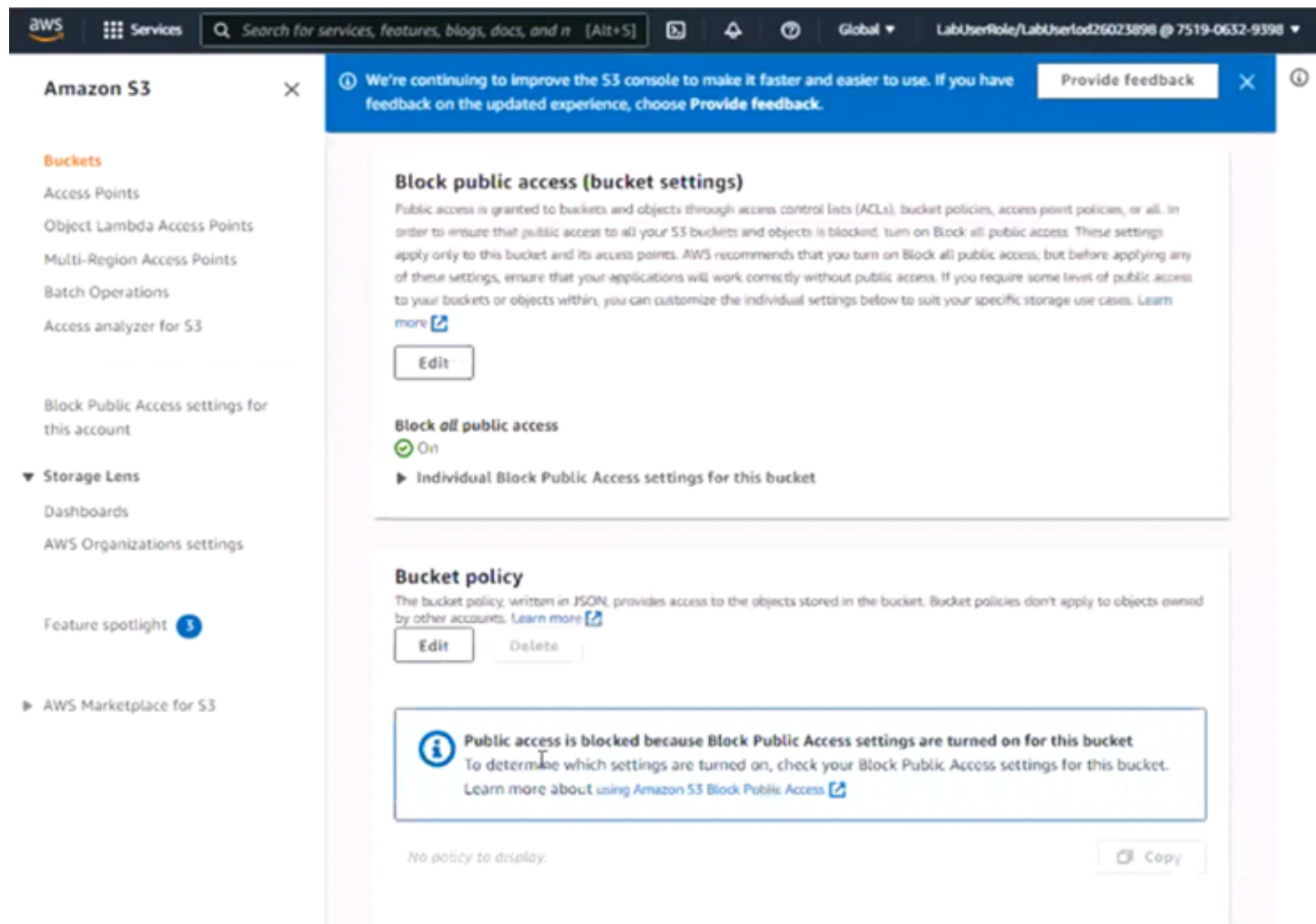
Note:

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

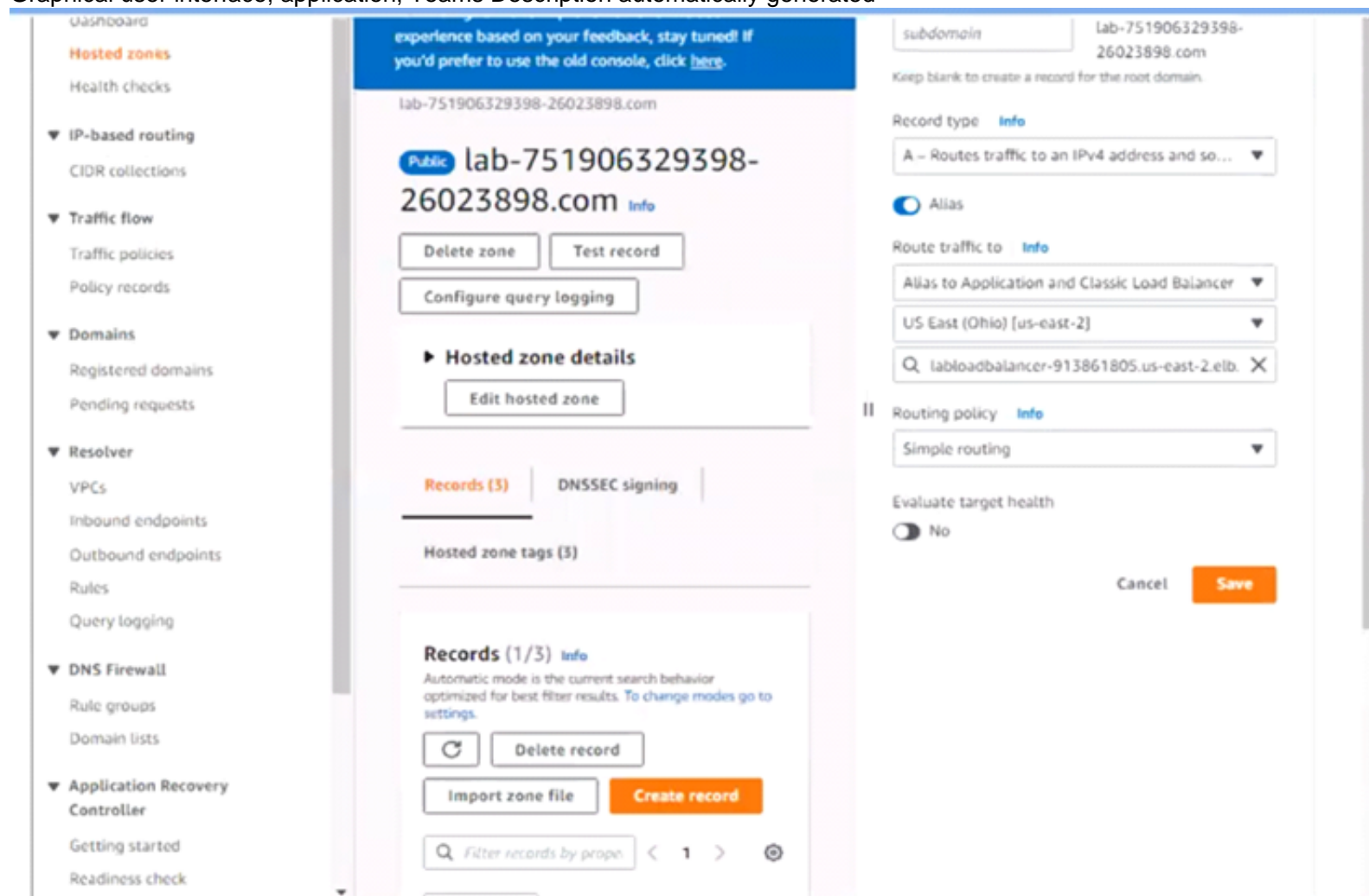


The screenshot displays the AWS Management Console interface. At the top, the 'Recently visited' section shows a cube icon and the text 'No recently visited services'. Below this, a list of commonly visited services is shown: IAM, EC2, S3, RDS, and Lambda. The 'Welcome to AWS' section on the left includes links for 'Getting started with AWS', 'Training and certification', and 'What's new with AWS?'. The 'AWS Health' section on the right shows a heart icon and the text 'No health data'. The main content area shows the 'Amazon S3' console, which includes a 'Buckets' section with an 'Account snapshot' and a table of buckets. The table has columns for Name, AWS Region, Access, and Creation date. A single bucket is listed with the name 'lab-751906329398-26023898.com', region 'US East (Ohio) us-east-2', and creation date 'September 30, 2022, 0'.

Graphical user interface, text, application Description automatically generated



Graphical user interface, application, Teams Description automatically generated




Graphical user interface, text, application Description automatically generated

The top screenshot displays the AWS Route 53 console interface. On the left, a sidebar lists navigation options: Dashboard, Hosted zones, Health checks, IP-based routing, Traffic flow, Domains, Resolver, and DNS Firewall. The main content area shows the 'Edit record' modal for a hosted zone named 'lab-751906329398-26023898.com'. The modal includes fields for 'Record name' (subdomain), 'Record type' (A - Routes traffic to an IPv4 address and so...), 'Route traffic to' (Alias to Application and Classic Load Balancer), and 'Routing policy' (Simple routing). A 'Save' button is at the bottom right.

The bottom screenshot shows the 'Quick create record' form. It includes a 'Record name' field (subdomain), a 'Record type' dropdown (A - Routes traffic to an IPv4 address and some AWS resources), a 'Value' field (192.0.2.235), a 'TTL (seconds)' field (300), and a 'Routing policy' dropdown (Simple routing). A 'Switch to wizard' link is at the top right, and an 'Add another record' button is at the bottom right.

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

 Services

[Alt+S]

Global

LabUserRole/LabUserIod26023898 @ 7519-0632-9398

Introducing the new Route 53 console

We've redesigned the Route 53 console to make it easier to use. [Let us know what you think](#). We are continuing to make improvements to the user experience based on your feedback, stay tuned! If you'd prefer to use the old console, click [here](#).

A – Routes traffic to an IPv4 address and some AWS resources ...

Keep blank to create a record for the root domain.

☐ Alias

Value

Info

Enter multiple values on separate lines.

TTL (seconds)

Info

Recommended values: 60 to 172800 (two days)

Routing policy

Info

Simple routing

Add another record

Cancel

Create records

View existing records

The following table lists the existing records in lab-751906329398-26023898.com.

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

A – Routes traffic to an IPv4 address and some AWS resources

☒ Alias

Route traffic to

Info

Alias to another record in this hosted zone

US East (N. Virginia)

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

X

Alias hosted zone ID: Z09119752YCYFLS823AF

Routing policy

Info


Failover

Failover record type

Secondary

Health check ID - optional

Info



Evaluate target health

☒ Yes

Record ID

Info

Add another record

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>

we've redesigned the Route 53 console to make it easier to use. [Learn more](#)

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](#)

subdomain lab-751906329398-26023898.com

Keep blank to create a record for the root domain.

Record type [Info](#)

A - Routes traffic to an IPv4 address and som...

☒ Alias

Route traffic to [Info](#)

Alias to another record in this hosted zone

US East (N. Virginia)

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


lab-751906329398-26023898.com

Alias hosted zone ID: Z09119752YCYFLS823AF

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

[Learn more](#)

[Working with records](#)

 Services [Alt+S]

Global LabUserRole/LabUserIod26023898 @ 7519-0632-9398

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

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

▼ Record 1 [Delete](#)

Record name [Info](#)

subdomain lab-751906329398-26023898.com

Keep blank to create a record for the root domain.

Record type [Info](#)

A - Routes traffic to an IPv4 address and some AWS resources

☒ Alias

Route traffic to [Info](#)

Alias to Application and Classic Load Balancer

US East (Ohio) [us-east-2]

dualstack.LabLoadBalancer-913861805.us-east-2.elb.amazonaws.com

Alias hosted zone ID: Z3AADJGX6KTTL2

Routing policy [Info](#)

Failover

Failover record type

Secondary

Health check ID - optional [Info](#)

f34f14a2-fe96-4fe0-8793-6e26cec223aa

Evaluate target health

☒ Yes

Record ID [Info](#)

sec

[Add another record](#)

NEW QUESTION 316

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SOA-C02 Practice Exam Features:

- * SOA-C02 Questions and Answers Updated Frequently
- * SOA-C02 Practice Questions Verified by Expert Senior Certified Staff
- * SOA-C02 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SOA-C02 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SOA-C02 Practice Test Here](#)