

Exam Questions SOA-C02

AWS Certified SysOps Administrator - Associate (SOA-C02)

<https://www.2passeasy.com/dumps/SOA-C02/>



NEW QUESTION 1

- (Exam Topic 1)

A SysOps administrator has used AWS Cloud Formation to deploy a sereness application into a production VPC. The application consists of an AWS Lambda function, an Amazon DynamoDB table, and an Amazon API Gateway API. The SysOps administrator must delete the AWS Cloud Formation stack without deleting the DynamoDB table.

Which action should the SysOps administrator take before deleting the AWS Cloud Formation stack?

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

Answer: A

NEW QUESTION 2

- (Exam Topic 1)

A company has an application that is running on Amazon EC2 instances in a VPC. The application needs access to download software updates from the internet. The VPC has public subnets and private signets. The company's security policy requires all ECS instances to be deployed in private subnets. What should a SysOps administrator do to meet those requirements?

- A. Add an internet gateway to the VPC In the route table for the private subnets, odd a route to the interne; gateway.
- B. Add a NAT gateway to a private subne
- C. In the route table for the private subnets, add a route to the NAT gateway.
- D. Add a NAT gateway to a public subnet in the route table for the private subnets, add a route to the NAT gateway.
- E. Add two internet gateways to the VP
- F. In The route tablet for the private subnets and public subnets, add a route to each internet gateway.

Answer: C

NEW QUESTION 3

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 4

- (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 5

- (Exam Topic 1)

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

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

- J. Within the policy, configure a weight of 80 for the record pointing to the original resource.
- K. Configure a weight of 20 for the record pointing to the new resource.

Answer: C

NEW QUESTION 6

- (Exam Topic 1)

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

A SysOps administrator must identify the top five internet destinations that the EC2 instances in the private subnet communicate with for downloads. What should the SysOps administrator do to meet this requirement in the MOST operationally efficient way?

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

Answer: C

NEW QUESTION 7

- (Exam Topic 1)

A SysOps administrator noticed that the cache hit ratio for an Amazon CloudFront distribution is less than 10%. Which collection of configuration changes will increase the cache hit ratio for the distribution? (Select TWO.)

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

Answer: AE

Explanation:

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

NEW QUESTION 8

- (Exam Topic 1)

A company is running a website on Amazon EC2 instances behind an Application Load Balancer (ALB). The company configured an Amazon CloudFront distribution and set the ALB as the origin. The company created an Amazon Route 53 CNAME record to send all traffic through the CloudFront distribution. As an unintended side effect, mobile users are now being served the desktop version of the website.

Which action should a SysOps administrator take to resolve this issue?

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

Answer: A

Explanation:

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

NEW QUESTION 9

- (Exam Topic 1)

A company stores its data in an Amazon S3 bucket. The company is required to classify the data and find any sensitive personal information in its S3 files. Which solution will meet these requirements?

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

Answer: D

Explanation:

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

NEW QUESTION 10

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 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 11

- (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 16

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

Answer: C

NEW QUESTION 19

- (Exam Topic 1)

A company has an existing web application that runs on two Amazon EC2 instances behind an Application Load Balancer (ALB) across two Availability Zones. The application uses an Amazon RDS Multi-AZ DB Instance. Amazon Route 53 record sets route requests for dynamic content to the load balancer and requests for static content to an Amazon S3 bucket. Site visitors are reporting extremely long loading times.

Which actions should be taken to improve the performance of the website? (Select TWO.)

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

Answer: AD

NEW QUESTION 21

- (Exam Topic 1)

A company needs to implement a managed file system to host Windows file shares for users on premises. Resources in the AWS Cloud also need access to the data on these file shares. A SysOps administrator needs to present the user file shares on premises and make the user file shares available on AWS with minimum latency.

What should the SysOps administrator do to meet these requirements?

- A. Set up an Amazon S3 File Gateway.
- B. Set up an AWS Direct Connect connection.
- C. Use AWS DataSync to automate data transfers between the existing file servers and AWS.
- D. Set up an Amazon FSx File Gateway.

Answer: D

Explanation:

Amazon FSx provides a fully managed file system that is optimized for Windows-based workloads and can be used to create file shares that can be accessed both on premises and in the AWS Cloud. The file shares that are created in Amazon FSx are highly available and can be accessed with low latency. Additionally, Amazon FSx supports Windows-based authentication, making it easy to integrate with existing Windows user accounts.

References:

[1] <https://aws.amazon.com/fsx/>

[2] <https://aws.amazon.com/storage/file-storage/>

[3] <https://docs.aws.a>

NEW QUESTION 23

- (Exam Topic 1)

A SysOps administrator must create an IAM policy for a developer who needs access to specific AWS services. Based on the requirements, the SysOps administrator creates the following policy:

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

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

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

Answer: DE

NEW QUESTION 25

- (Exam Topic 1)

A SysOps administrator has created a VPC that contains a public subnet and a private subnet. Amazon EC2 instances that were launched in the private subnet cannot access the internet. The default network ACL is active on all subnets in the VPC, and all security groups allow all outbound traffic:

Which solution will provide the EC2 instances in the private subnet with access to the internet?

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

Answer: A

Explanation:

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

NEW QUESTION 29

- (Exam Topic 1)

A company recently its server infrastructure to Amazon EC2 instances. The company wants to use Amazon CloudWatch metrics to track instance memory utilization and available disk space.

What should a SysOps administrator do to meet these requirements?

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

Answer: C

NEW QUESTION 32

- (Exam Topic 1)

A company wants to build a solution for its business-critical Amazon RDS for MySQL database. The database requires high availability across different geographic locations. A SysOps administrator must build a solution to handle a disaster recovery (DR) scenario with the lowest recovery time objective (RTO) and recovery point objective (RPO).

Which solution meets these requirements?

- A. Create automated snapshots of the database on a schedul
- B. Copy the snapshots to the DR Region.
- C. Create a cross-Region read replica for the database.
- D. Create a Multi-AZ read replica for the database.
- E. Schedule AWS Lambda functions to create snapshots of the source database and to copy the snapshots to a DR Region.

Answer: B

NEW QUESTION 35

- (Exam Topic 1)

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

- A. Create an AWS Config rule to detect noncompliant security group
- B. Set up automatic remediation to change the 0.0.0.0/0 source address to the approved CIDK block.
- C. Create an IAM policy to deny the creation of security groups that have 0.0.0.0/0 as the source address Attach this 1AM policy to every user in the company.
- D. Create an AWS Lambda function to inspect now and existing security groups check for a noncompliant 0.0.0.0A) source address and change the source address to the approved CIDR block.
- E. Create a service control policy (SCP) for the organizational unit (OU) to deny the creation of security groups that have the 0.0.0.0/0 source addres
- F. Set up automatic remediation to change Vie 0.0.0.0/0 source address to the approved CIDR block.

Answer: A

NEW QUESTION 38

- (Exam Topic 1)

A company uses an Amazon S3 bucket to store data files. The S3 bucket contains hundreds of objects. The company needs to replace a tag on all the objects in the S3 bucket with another tag.

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

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

Answer: A

Explanation:

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

NEW QUESTION 40

- (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 42

- (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 45

- (Exam Topic 1)

A company is hosting applications on Amazon EC2 instances. The company is hosting a database on an Amazon RDS for PostgreSQL DB instance. The company requires all connections to the DB instance to be encrypted.

What should a SysOps administrator do to meet this requirement?

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

Answer: C

Explanation:

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

NEW QUESTION 47

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 49

- (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 53

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 56

- (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 57

- (Exam Topic 1)

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

What change should be made to alleviate the performance problem?

- A. Change the Amazon EBS volume to Provisioned IOPs
- B. Upgrade to a compute-optimized instance
- C. Add additional 12 large instances to the application
- D. Purchase Reserved Instances

Answer: B

NEW QUESTION 59

- (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 60

- (Exam Topic 1)

A SysOps administrator Is troubleshooting an AWS Cloud Formation 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 Cloud Formation 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 CloudFormaton template to specify the region code as part of the fully qualified AMI ID.
- C. Edit the AWS CloudFormaton 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" sectio
- E. Refer to the proper mapping within the template for the proper AMI ID.

Answer: A

NEW QUESTION 64

- (Exam Topic 1)

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

Which solution will meet this requirement?

- A. Assess AWS CloudTrail logs to verify that there is no EC2 API activit

- B. Invoke an AWS Lambda function to stop the EC2 instances.
- C. Create an Amazon CloudWatch alarm to stop the EC2 instances when the average CPU utilization is lower than 5% for a 30-minute period.
- D. Create an Amazon CloudWatch metric to stop the EC2 instances when the VolumeReadBytes metric is lower than 500 for a 30-minute period.
- E. Use AWS Config to invoke an AWS Lambda function to stop the EC2 instances based on resource configuration changes.

Answer: B

Explanation:

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

NEW QUESTION 66

- (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 68

- (Exam Topic 1)

A SysOps administrator must create a solution that automatically shuts down any Amazon EC2 instances that have less than 10% average CPU utilization for 60 minutes or more.

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

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

Answer: B

Explanation:

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

NEW QUESTION 72

- (Exam Topic 1)

A user working in the Amazon EC2 console increased the size of an Amazon Elastic Block Store (Amazon EBS) volume attached to an Amazon EC2 Windows instance. The change is not reflected in the file system.

What should a SysOps administrator do to resolve this issue?

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

Answer: B

NEW QUESTION 77

- (Exam Topic 1)

A company's application currently uses an IAM role that allows all access to all AWS services. A SysOps administrator must ensure that the company's IAM policies allow only the permissions that the application requires.

How can the SysOps administrator create a policy to meet this requirement?

- A. Turn on AWS CloudTrail.
- B. Generate a policy by using AWS Security Hub.
- C. Turn on Amazon EventBridge (Amazon CloudWatch Events). Generate a policy by using AWS Identity and Access Management Access Analyzer.
- D. Use the AWS CLI to run the get-generated-policy command in AWS Identity and Access Management Access Analyzer.
- E. Turn on AWS CloudTrail.
- F. Generate a policy by using AWS Identity and Access Management Access Analyzer.

Answer: D

Explanation:

Generate a policy by using AWS Identity and Access Management Access Analyzer. AWS CloudTrail is a service that records all API calls made on your account. You can use this data to generate a policy with AWS Identity and Access Management Access Analyzer that only allows the permissions that the application requires. This will ensure that the application only has the necessary permissions and will protect the company from any unauthorized access.

<https://docs.aws.amazon.com/IAM/latest/UserGuide/what-is-access-analyzer.html#what-is-access-analyzer-poli>

NEW QUESTION 79

- (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 83

- (Exam Topic 1)

A Sysops administrator has created an Amazon EC2 instance using an AWS CloudFormation template in the us-east-1 Region. The administrator finds that this template has failed to create an EC2 instance in the us-west-2 Region. What is one cause for this failure?

- A. Resource tags defined in the CloudFormation template are specific to the us-east-1 Region.
- B. The Amazon Machine Image (AMI) ID referenced in the CloudFormation template could not be found in the us-west-2 Region.
- C. The cfn-init script did not run during resource provisioning in the us-west-2 Region.
- D. The IAM user was not created in the specified Region.

Answer: B

Explanation:

One possible cause for the failure of the CloudFormation template to create an EC2 instance in the us-west-2 Region is that the Amazon Machine Image (AMI) ID referenced in the template could not be found in the us-west-2 Region. This could be due to the fact that the AMI is not available in that region, or the credentials used to access the AMI were not configured properly. The other options (resource tags defined in the CloudFormation template are specific to the us-east-1 Region, the cfn-init script did not run during resource provisioning in the us-west-2 Region, and the IAM user was not created in the specified Region) are not valid causes for this failure.

NEW QUESTION 88

- (Exam Topic 1)

A company has mandated the use of multi-factor authentication (MFA) for all IAM users, and requires users to make all API calls using the CLI. However, users are not prompted to enter MFA tokens, and are able to run CLI commands without MFA. In an attempt to enforce MFA, the company attached an IAM policy to all users that denies API calls that have not been authenticated with MFA.

What additional step must be taken to ensure that API calls are authenticated using MFA?

- A. Enable MFA on IAM roles, and require IAM users to use role credentials to sign API calls.
- B. Ask the IAM users to log into the AWS Management Console with MFA before making API calls using the CLI.
- C. Restrict the IAM users to use of the console, as MFA is not supported for CLI use.
- D. Require users to use temporary credentials from the get-session token command to sign API calls.

Answer: D

NEW QUESTION 93

- (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 98

- (Exam Topic 1)

A company hosts a web application on an Amazon EC2 instance. The web server logs are published to Amazon CloudWatch Logs. The log events have the same structure and include the HTTP response codes that are associated with the user requests. The company needs to monitor the number of times that the web server returns an HTTP 404 response.

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

- A. Create a CloudWatch Logs metric filter that counts the number of times that the web server returns an HTTP 404 response.
- B. Create a CloudWatch Logs subscription filter that counts the number of times that the web server returns an HTTP 404 response.
- C. Create an AWS Lambda function that runs a CloudWatch Logs Insights query that counts the number of 404 codes in the log events during the past hour.
- D. Create a script that runs a CloudWatch Logs Insights query that counts the number of 404 codes in the log events during the past hour.

Answer: A

Explanation:

This is the most operationally efficient solution that meets the requirements, as it will allow the company to monitor the number of times that the web server returns an HTTP 404 response in real-time. The other solutions (creating a CloudWatch Logs subscription filter, an AWS Lambda function, or a script) will require additional steps and resources to monitor the number of times that the web server returns an HTTP 404 response.

A metric filter allows you to search for specific terms, phrases, or values in your log events, and then to create a metric based on the number of occurrences of those search terms. This allows you to create a CloudWatch Metric that can be used to create alarms and dashboards, which can be used to monitor the number of HTTP 404 responses returned by the web server.

NEW QUESTION 99

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 102

- (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

NEW QUESTION 104

- (Exam Topic 1)

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

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

Answer: DE

NEW QUESTION 109

- (Exam Topic 1)

A company has an application that customers use to search for records on a website. The application's data is stored in an Amazon Aurora DB cluster. The application's usage varies by season and by day of the week.

The website's popularity is increasing, and the website is experiencing slower performance because of increased load on the DB cluster during periods of peak activity. The application logs show that the performance issues occur when users are searching for information. The same search is rarely performed multiple times.

A SysOps administrator must improve the performance of the platform by using a solution that maximizes resource efficiency. Which solution will meet these requirements?

- A. Deploy an Amazon ElastiCache for Redis cluster in front of the DB cluster.
- B. Modify the application to check the cache before the application issues new queries to the database.
- C. Add the results of any queries to the cache.
- D. Deploy an Aurora Replica for the DB cluster.
- E. Modify the application to use the reader endpoint for search operation.
- F. Use Aurora Auto Scaling to scale the number of replicas based on load.
- G. Most Voted.
- H. Use Provisioned IOPS on the storage volumes that support the DB cluster to improve performance sufficiently to support the peak load on the application.
- I. Increase the instance size in the DB cluster to a size that is sufficient to support the peak load on the application.
- J. Use Aurora Auto Scaling to scale the instance size based on load.

Answer: B

Explanation:

https://docs.amazonaws.cn/en_us/AmazonRDS/latest/AuroraUserGuide/aurora-replicas-adding.html

NEW QUESTION 111

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

Answer: B

Explanation:

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

NEW QUESTION 116

- (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 117

- (Exam Topic 1)

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

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

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

Answer: C

NEW QUESTION 118

- (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 123

- (Exam Topic 1)

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

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

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

Answer: CD

Explanation:

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

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

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

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

NEW QUESTION 127

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 132

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

Answer: C

NEW QUESTION 133

- (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/RDP.
- F. Export the database contents into a file, then share this file with the other accounts.

Answer: B

NEW QUESTION 134

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 138

- (Exam Topic 1)

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

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

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

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

Answer: B

Explanation:

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

NEW QUESTION 141

- (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 145

- (Exam Topic 1)

A company has a public website that recently experienced problems. Some links led to missing webpages, and other links rendered incorrect webpages. The application infrastructure was running properly, and all the provisioned resources were healthy. Application logs and dashboards did not show any errors, and no monitoring alarms were raised. Systems administrators were not aware of any problems until end users reported the issues.

The company needs to proactively monitor the website for such issues in the future and must implement a solution as soon as possible.

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

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

Answer: A

NEW QUESTION 147

- (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 148

- (Exam Topic 1)

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

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

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

Answer: B

NEW QUESTION 151

- (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 `host1.awscloud.private`. An AWS Site-to-Site VPN connection is in place between the on-premises network and AWS.

The application that runs in the data center tries to connect to the application that runs on the EC2 instance, but DNS resolution fails. A SysOps administrator must implement DNS resolution between 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 152

- (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 156

- (Exam Topic 1)

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

Which solution meets these requirements?

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

Answer: B

NEW QUESTION 158

- (Exam Topic 1)

A SysOps administrator is setting up a fleet of Amazon EC2 instances in an Auto Scaling group for an application. The fleet should have 50% CPU available at that times to accommodate bursts of traffic. The load will increase significantly between the hours of 09:00 and 17:00, 7 days a week

How should the SysOps administrator configure the scaling of the EC2 instances to meet these requirements?

- A. Create a target tracking scaling policy that runs when the CPU utilization is higher than 90%
- B. Create a target tracking scaling policy that runs when the CPU utilization is higher than 50%. Create a scheduled scaling policy that ensures that the fleet is

available at 09:00 Create a second scheduled scaling policy that scales in the fleet at 17:00

C. Set the Auto Scaling group to start with 2 instances by setting the desired instances maximum instances, and minimum instances to 2 Create a scheduled scaling policy that ensures that the fleet is available at 09:00

D. Create a scheduled scaling policy that ensures that the fleet is available at 09.00. Create a second scheduled scaling policy that scales in the fleet at 17:00

Answer: B

NEW QUESTION 163

- (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-aw>

NEW QUESTION 164

- (Exam Topic 1)

A SysOps Administrator runs a web application that is using a microservices approach whereby different responsibilities of the application have been divided in a separate microservice running on a different Amazon EC2 instance. The administrator has been tasked with reconfiguring the infrastructure to support this approach.

How can the administrator accomplish this with the LEAST administrative overhead?

A. Use Amazon CloudFront to log the URL and forward the request.

B. Use Amazon CloudFront to rewrite the header based on the microservice and forward the request.

C. Use an Application Load Balancer (ALB) and do path-based routing.

D. Use a Network Load Balancer (NLB) and do path-based routing.

Answer: C

Explanation:

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

NEW QUESTION 165

- (Exam Topic 1)

A company runs hundreds of Amazon EC2 instances in a single AWS Region. Each EC2 instance has two attached 1 GiB General Purpose SSD (gp2) Amazon Elastic Block Store (Amazon EBS) volumes. A critical workload is using all the available IOPS capacity on the EBS volumes.

According to company policy, the company cannot change instance types or EBS volume types without completing lengthy acceptance tests to validate that the company's applications will function properly. A SysOps administrator needs to increase the I/O performance of the EBS volumes as quickly as possible.

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

A. Increase the size of the 1 GiB EBS volumes.

B. Add two additional elastic network interfaces on each EC2 instance.

C. Turn on Transfer Acceleration on the EBS volumes in the Region.

D. Add all the EC2 instances to a cluster placement group.

Answer: A

Explanation:

Increasing the size of the 1 GiB EBS volumes will increase the IOPS capacity of the volumes, which will improve the I/O performance of the EBS volumes. This option does not require any changes to the instance types or EBS volume types, so it can be done quickly without the need for lengthy acceptance tests to validate that the company's applications will function properly.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/requesting-ebs-volume-modifications.html>

NEW QUESTION 166

- (Exam Topic 1)

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

A. AWS Config

B. Amazon Inspector

C. AWS Trusted Advisor

D. AWS Systems Manager

Answer: D

NEW QUESTION 167

- (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 170

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 175

- (Exam Topic 1)

A SysOps administrator is helping a development team deploy an application to AWS. The AWS CloudFormation template includes an Amazon Linux EC2 Instance, an Amazon Aurora DB cluster, and a hard-coded database password that must be rotated every 90 days. What is the MOST secure way to manage the database password?

- A. Use the AWS SecretsManager Secret resource with the GenerateSecretString property to automatically generate a password. Use the AWS SecretsManager RotationSchedule resource to define a rotation schedule for the password. Configure the application to retrieve the secret from AWS Secrets Manager, access the database.
- B. Use the AWS SecretsManager Secret resource with the SecretString property. Accept a password as a CloudFormation parameter. Use the AllowedPattern property of the CloudFormation parameter to require a minimum length, uppercase and lowercase letters, and special characters. Configure the application to retrieve the secret from AWS Secrets Manager to access the database.
- C. Use the AWS SSM Parameter resource. Accept input as a CloudFormation parameter to store the parameter as a secure string. Configure the application to retrieve the parameter from AWS Systems Manager Parameter Store to access the database.
- D. Use the AWS SSM Parameter resource. Accept input as a CloudFormation parameter to store the parameter as a string. Configure the application to retrieve the parameter from AWS Systems Manager Parameter Store to access the database.

Answer: A

NEW QUESTION 176

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 180

- (Exam Topic 1)

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

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

Answer: AE

NEW QUESTION 185

- (Exam Topic 1)

A company has a web application with a database tier that consists of an Amazon EC2 instance that runs MySQL. A SysOps administrator needs to minimize potential data loss and the time that is required to recover in the event of a database failure.

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

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

Answer: D

NEW QUESTION 187

- (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 bucke
- 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 da
- J. Configure the cron job to send a notification if an item is missing.

Answer: A

Explanation:

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

NEW QUESTION 188

- (Exam Topic 1)

Application A runs on Amazon EC2 instances behind a Network Load Balancer (NLB). The EC2 instances are in an Auto Scaling group and are in the same subnet that is associated with the NLB. Other applications from an on-premises environment cannot communicate with Application A on port 8080.

To troubleshoot the issue, a SysOps administrator analyzes the flow logs. The flow logs include the following records:

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

What is the reason for the rejected traffic?

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

Answer: A

NEW QUESTION 193

- (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 198

- (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 CloudWatc
- 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 202

- (Exam Topic 1)

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

What is the MOST scalable storage solution to fulfill this requirement?

- A. Connect a large Amazon EBS volume to multiple instances and schedule snapshots.
- B. Deploy Amazon EFS in the VPC and create mount targets in multiple subnets.
- C. Launch an EC2 instance and share data using SMB/CIFS or NFS.
- D. Deploy an AWS Storage Gateway cached volume on Amazon EC2.

Answer: B

NEW QUESTION 205

- (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 ke
- 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 encryptio
- F. Enable encryption in the CloudFront distribution, and use the S3 bucket as a log destination.

Answer: C

NEW QUESTION 206

- (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 211

- (Exam Topic 1)

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

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

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

Answer: D

NEW QUESTION 214

- (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 217

- (Exam Topic 1)

A SysOps administrator has launched a large general purpose Amazon EC2 instance to regularly process large data files. The instance has an attached 1 TB General Purpose SSD (gp2) Amazon Elastic Block Store (Amazon EBS) volume. The instance also is EBS-optimized. To save costs, the SysOps administrator stops the instance each evening and restarts the instance each morning.

When data processing is active, Amazon CloudWatch metrics on the instance show a consistent 3.000 VolumeReadOps. The SysOps administrator must improve the I/O performance while ensuring data integrity.

Which action will meet these requirements?

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

Answer: C

NEW QUESTION 222

- (Exam Topic 1)

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

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

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

Answer: D

NEW QUESTION 224

- (Exam Topic 1)

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

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

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

Answer: B

Explanation:

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

NEW QUESTION 225

- (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 226

- (Exam Topic 1)

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

What must the SysOps administrator do to resolve this issue?

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

Answer: D

NEW QUESTION 227

- (Exam Topic 1)

A SysOps administrator configures an Amazon S3 gateway endpoint in a VPC. The private subnets inside the VPC do not have outbound internet access. A user logs in to an Amazon EC2 instance in one of the private subnets and cannot upload a file to an Amazon S3 bucket in the same AWS Region

Which solution will solve this problem?

- A. Update the EC2 instance role policy to allow s3:PutObject access to the target S3 bucket.
- B. Update the EC2 security group to allow outbound traffic to 0.0.0.0/0 for port 80.
- C. Update the EC2 subnet route table to include the S3 prefix list destination routes to the S3 gateway endpoint.
- D. Update the S3 bucket policy to allow s3:PutObject access from the private subnet CIDR block.

Answer: C

NEW QUESTION 231

- (Exam Topic 1)

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

What should the SysOps administrator do to resolve this issue?

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

Answer: D

NEW QUESTION 234

- (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 239

- (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 243

- (Exam Topic 1)

A company must migrate its applications to AWS. The company is using Chef recipes for configuration management. The company wants to continue to use the existing Chef recipes after the applications are migrated to AWS.

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

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

Answer: D

NEW QUESTION 248

- (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 253

- (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 258

- (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 262

- (Exam Topic 1)

A company has attached the following policy to an IAM user:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "rds:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:Region": "us-east-1"
        }
      }
    },
    {
      "Effect": "Deny",
      "NotAction": [
        "ec2:*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:Region": "us-east-1"
        }
      }
    },
    {
      "Effect": "Deny",
      "NotAction": [
        "ec2:*",
        "s3:GetObject"
      ],
      "Resource": "*"
    }
  ]
}
```

Which of the following actions are allowed for the IAM user?

- A. Amazon RDS DescribeDBInstances action in the us-east-1 Region
- B. Amazon S3 Putobject operation in a bucket named testbucket
- C. Amazon EC2 Describe Instances action in the us-east-1 Region
- D. Amazon EC2 AttachNetworkinterface action in the eu-west-1 Region

Answer: C

NEW QUESTION 263

- (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 metric
- 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 period

- 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) rule
- 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 266

- (Exam Topic 1)

A company is managing multiple AWS accounts in AWS Organizations. The company is reviewing internal security of its AWS environment. The company's security administrator has their own AWS account and wants to review the VPC configuration of developer AWS accounts. Which solution will meet these requirements in the MOST secure manner?

- A. Create an IAM policy in each developer account that has read-only access related to VPC resources. Assign the policy to an IAM user. Share the user credentials with the security administrator.
- B. Create an IAM policy in each developer account that has administrator access to all Amazon EC2 actions, including VPC actions. Assign the policy to an IAM user. Share the user credentials with the security administrator.
- C. Create an IAM policy in each developer account that has administrator access related to VPC resources. Assign the policy to a cross-account IAM role. Ask the security administrator to assume the role from their account.
- D. Create an IAM policy in each developer account that has read-only access related to VPC resources. Assign the policy to a cross-account IAM role. Ask the security administrator to assume the role from their account.

Answer: D

NEW QUESTION 269

- (Exam Topic 1)

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

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

Answer: AD

Explanation:

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

NEW QUESTION 273

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 278

- (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 lo
- E. Set the log record format to a custom format Select the proper fields to include in the tog

Answer: A

NEW QUESTION 280

- (Exam Topic 1)

An AWS Lambda function is intermittently failing several times a day A SysOps administrator must find out how often this error has occurred in the last 7 days Which action will meet this requirement in the MOST operationally efficient manner?

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

Answer: C

NEW QUESTION 282

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 286

- (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 287

- (Exam Topic 1)

A company's SysOps administrator deploys a public Network Load Balancer (NLB) in front of the company's web application. The web application does not use any Elastic IP addresses. Users must access the web application by using the company's domain name. The SysOps administrator needs to configure Amazon Route 53 to route traffic to the NLB.

Which solution will meet these requirements MOST cost-effectively?

- A. Create a Route 53 AAAA record for the NLB.
- B. Create a Route 53 alias record for the NLB.
- C. Create a Route 53 CAA record for the NLB.
- D. Create a Route 53 CNAME record for the NLB.

Answer: B

NEW QUESTION 288

- (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 293

- (Exam Topic 1)

A SysOps administrator needs to design a high-traffic static website. The website must be highly available and must provide the lowest possible latency to users across the globe.

Which solution will meet these requirements?

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

Answer: B

NEW QUESTION 296

- (Exam Topic 1)

A company has a new requirement stating that all resources in AWS must be tagged according to a set policy. Which AWS service should be used to enforce and continually identify all resources that are not in compliance with the policy?

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

Answer: C

NEW QUESTION 300

- (Exam Topic 1)

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

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

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

Answer: C

NEW QUESTION 304

- (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 308

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 310

- (Exam Topic 1)

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

Which configuration will meet these requirements?

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

Answer: B

Explanation:

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

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

https://en.wikipedia.org/wiki/SOA_record

NEW QUESTION 312

- (Exam Topic 1)

A company recently migrated its application to a VPC on AWS. An AWS Site-to-Site VPN connection connects the company's on-premises network to the VPC. The application retrieves customer data from another system that resides on premises. The application uses an on-premises DNS server to resolve domain records. After the migration, the application is not able to connect to the customer data because of name resolution errors.

Which solution will give the application the ability to resolve the internal domain names?

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

Answer: B

Explanation:

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

NEW QUESTION 313

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

Answer: C

NEW QUESTION 315

- (Exam Topic 1)

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

What could be the reason for this issue?

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

Answer: C

NEW QUESTION 320

- (Exam Topic 1)

A company hosts an online shopping portal in the AWS Cloud. The portal provides HTTPS security by using a TLS certificate on an Elastic Load Balancer (ELB). Recently, the portal suffered an outage because the TLS certificate expired. A SysOps administrator must create a solution to automatically renew certificates to avoid this issue in the future.

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

- A. Request a public certificate by using AWS Certificate Manager (ACM). Associate the certificate from ACM with the EL
- B. Write a scheduled AWS Lambda function to renew the certificate every 18 months.
- C. Request a public certificate by using AWS Certificate Manager (ACM). Associate the certificate from ACM with the EL
- D. ACM will automatically manage the renewal of the certificate.
- E. Register a certificate with a third-party certificate authority (CA). Import this certificate into AWS Certificate Manager (ACM). Associate the certificate from ACM with the EL
- F. ACM will automatically manage the renewal of the certificate.
- G. Register a certificate with a third-party certificate authority (CA). Configure the ELB to import the certificate directly from the C
- H. Set the certificate refresh cycle on the ELB to refresh when the certificate is within 3 months of the expiration date.

Answer: B

Explanation:

"A certificate is eligible for automatic renewal subject to the following considerations: ELIGIBLE if associated with another AWS service, such as Elastic Load Balancing or CloudFront. ELIGIBLE if exported since being issued or last renewed. ELIGIBLE if it is a private certificate issued by calling the ACM RequestCertificate API and then exported or associated with another AWS service. ELIGIBLE if it is a private certificate issued through the management console and then exported or associated with another AWS service." <https://docs.aws.amazon.com/acm/latest/userguide/managed-renewal.html>

NEW QUESTION 324

- (Exam Topic 1)

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

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

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

Answer: C

Explanation:

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

NEW QUESTION 326

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SOA-C02 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SOA-C02 Product From:

<https://www.2passeasy.com/dumps/SOA-C02/>

Money Back Guarantee

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