

Amazon-Web-Services

Exam Questions SOA-C02

AWS Certified SysOps Administrator - Associate (SOA-C02)



NEW QUESTION 1

- (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 subnets. The company's security policy requires all EC2 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, add a route to the internet gateway.
- B. Add a NAT gateway to a private subnet.
- 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 VPC.
- F. In the route table for the private subnets and public subnets, add a route to each internet gateway.

Answer: C

NEW QUESTION 2

- (Exam Topic 1)

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

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

Answer: A

Explanation:

Using Amazon S3 Block Public Access

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

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

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

NEW QUESTION 3

- (Exam Topic 1)

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

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

What is the result of this policy?

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

Answer: B

NEW QUESTION 4

- (Exam Topic 1)

A company runs a website from Sydney, Australia. Users in the United States (US) and Europe are reporting that images and videos are taking a long time to load. However, local testing in Australia indicates no performance issues. The website has a large amount of static content in the form of images and videos that are stored in Amazon S3.

Which solution will result in the MOST improvement in the user experience for users in the US and Europe?

- A. Configure AWS PrivateLink for Amazon S3.
- B. Configure S3 Transfer Acceleration.
- C. Create an Amazon CloudFront distributio
- D. Distribute the static content to the CloudFront edge locations
- E. Create an Amazon API Gateway API in each AWS Regio
- F. Cache the content locally.

Answer: D

NEW QUESTION 5

- (Exam Topic 1)

A SysOps administrator is provisioning an Amazon Elastic File System (Amazon EFS) file system to provide shared storage across multiple Amazon EC2 instances. The instances all exist in the same VPC across multiple Availability Zones. There are two instances in each Availability Zone. The SysOps administrator must make the file system accessible to each instance with the lowest possible latency.

Which solution will meet these requirements?

- A. Create a mount target for the EFS file system in the VP
- B. Use the mount target to mount the file system on each of the instances
- C. Create a mount target for the EFS file system in one Availability Zone of the VP
- D. Use the mount target to mount the file system on the instances in that Availability Zon
- E. Share the directory with the other instances.
- F. Create a mount target for each instanc
- G. Use each mount target to mount the EFS file system on each respective instance.
- H. Create a mount target in each Availability Zone of the VPC. Use the mount target to mount the EFS file system on the instances in the respective Availability Zone.

Answer: D

Explanation:

A mount target provides an IP address for an NFSv4 endpoint at which you can mount an Amazon EFS file system. You mount your file system using its Domain Name Service (DNS) name, which resolves to the IP address of the EFS mount target in the same Availability Zone as your EC2 instance. You can create one mount target in each Availability Zone in an AWS Region. If there are multiple subnets in an Availability Zone in your VPC, you create a mount target in one of the subnets. Then all EC2 instances in that Availability Zone share that mount target. <https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html>

NEW QUESTION 6

- (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 7

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 8

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 9

- (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 10

- (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 10

- (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 15

- (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 object.
- H. Save the tags in a list.
- 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 bucket.
- 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 16

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 19

- (Exam Topic 1)

A company with multiple AWS accounts needs to obtain recommendations for AWS Lambda functions and identify optimal resource configurations for each Lambda function. How should a SysOps administrator provide these recommendations?

- A. Create an AWS Serverless Application Repository and export the Lambda function recommendations.
- B. Enable AWS Compute Optimizer and export the Lambda function recommendations.
- C. Enable all features of AWS Organization and export the recommendations from AWS CloudTrail Insights.
- D. Run AWS Trusted Advisor and export the Lambda function recommendations.

Answer: B

NEW QUESTION 21

- (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 22

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 27

- (Exam Topic 1)

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

Where can the administrator find this information?

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

Answer: D

Explanation:

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

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

NEW QUESTION 31

- (Exam Topic 1)

A SysOps administrator created an Amazon VPC with an IPv6 CIDR block, which requires access to the internet. However, access from the internet towards the VPC is prohibited. After adding and configuring the required components to the VPC, the administrator is unable to connect to any of the domains that reside on the internet.

What additional route destination rule should the administrator add to the route tables?

- A. Route ::/0 traffic to a NAT gateway
- B. Route ::/0 traffic to an internet gateway
- C. Route 0.0.0.0/0 traffic to an egress-only internet gateway
- D. Route ::/0 traffic to an egress-only internet gateway

Answer: D

Explanation:

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

NEW QUESTION 32

- (Exam Topic 1)

A company's reporting job that used to run in 15 minutes is now taking an hour to run. An application generates the reports. The application runs on Amazon EC2 instances and extracts data from an Amazon RDS for MySQL database.

A SysOps administrator checks the Amazon CloudWatch dashboard for the RDS instance and notices that the Read IOPS metrics are high, even when the reports are not running. The SysOps administrator needs to improve the performance and the availability of the RDS instance.

Which solution will meet these requirements?

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

Answer: B

Explanation:

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

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

NEW QUESTION 35

- (Exam Topic 1)

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

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

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

Answer: A

NEW QUESTION 38

- (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 42

- (Exam Topic 1)

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

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

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

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

Answer: A

NEW QUESTION 46

- (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 51

- (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 53

- (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 58

- (Exam Topic 1)

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

- A. Add an additional node to the ElastiCache cluster.

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

Answer: AC

Explanation:

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

NEW QUESTION 60

- (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 61

- (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 64

- (Exam Topic 1)

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

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

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

Answer: AD

NEW QUESTION 68

- (Exam Topic 1)

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

What should the SysOps administrator do to meet these requirements?

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

Answer: C

Explanation:

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

NEW QUESTION 70

- (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 Synthetics canary
- G. Use the CloudWatch Synthetics 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 74

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 75

- (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 80

- (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 85

- (Exam Topic 1)

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

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

What should a SysOps administrator do to resolve this error?

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

Answer: D

NEW QUESTION 87

- (Exam Topic 1)

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

What should the SysOps administrator do to sign in?

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

Answer: A

NEW QUESTION 89

- (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 94

- (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 aws-vpc 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 97

- (Exam Topic 1)

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

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

What should a SysOps administrator do to resolve this problem?

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

Answer: A

Explanation:

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

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

There's an SSL negotiation failure because the SSL certificate on the origin is expired or invalid, or because the certificate chain is invalid.
There's a host header mismatch in the SSL negotiation between your CloudFront distribution and the custom origin.
The custom origin isn't responding on the ports specified in the origin settings of the CloudFront distribution. The custom origin is ending the connection to CloudFront too quickly.
<https://aws.amazon.com/premiumsupport/knowledge-center/resolve-cloudfront-connection-error/>

NEW QUESTION 102

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

Answer: A

Explanation:

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

NEW QUESTION 106

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 108

- (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 113

- (Exam Topic 1)

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

What should the SysOps administrator do to meet this requirement?

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

- M. Update the S3 bucket policy to allow access only from the OA
- N. Disable website hostin
- O. Create a new origin, and specify the S3 bucket as the new origi
- P. Update the distribution behavior to use the new origi
- Q. Remove the existing origin.
- R. Update the S3 bucket policy to allow access only from the CloudFront distributio
- S. Remove access to and from other principals in the S3 bucket polic
- T. Disable website hostin
- . Create a new origin, and specify the S3 bucket as the new origi
- . Update the distribution behavior to use the new origi
- . Remove the existing origin.

Answer: A

NEW QUESTION 114

- (Exam Topic 1)

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 116

- (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:PutObjed 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 PurObject access from the private subnet CIDR block.

Answer: C

NEW QUESTION 121

- (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 Cloud Format ion to create an Amazon EC2 instance, install a Chef server, and add Chefrecipes.
- 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 126

- (Exam Topic 1)

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

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

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

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

Answer: C

NEW QUESTION 131

- (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 134

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 137

- (Exam Topic 1)

A team of on-call engineers frequently needs to connect to Amazon EC2 instances in a private subnet to troubleshoot and run commands. The instances use either the latest AWS-provided Windows Amazon Machine Images (AMIs) or Amazon Linux AMIs. The team has an existing IAM role for authorization. A SysOps administrator must provide the team with access to the instances by granting IAM permissions to this. Which solution will meet this requirement?

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

Answer: A

NEW QUESTION 140

- (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 143

- (Exam Topic 1)

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

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

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

Answer: DE

Explanation:

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

NEW QUESTION 144

- (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 146

- (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 149

- (Exam Topic 1)

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

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

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

Answer: A

NEW QUESTION 152

- (Exam Topic 1)

A company has a VPC with public and private subnets. An Amazon EC2 based application resides in the private subnets and needs to process raw .csv files stored in an Amazon S3 bucket. A SysOps administrator has set up the correct IAM role with the required permissions for the application to access the S3 bucket, but the application is unable to communicate with the S3 bucket.

Which action will solve this problem while adhering to least privilege access?

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

Answer: B

Explanation:

Technology to use is a VPC endpoint - "A VPC endpoint enables private connections between your VPC and supported AWS services and VPC endpoint services powered by AWS PrivateLink. AWS PrivateLink is a technology that enables you to privately access services by using private IP addresses. Traffic between your VPC and the other service does not leave the Amazon network." S3 is an example of a gateway endpoint. We want to see services in AWS while not leaving the VPC.

NEW QUESTION 156

- (Exam Topic 1)

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

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

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

Answer: C

NEW QUESTION 160

- (Exam Topic 1)

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

What should a SysOps administrator do to resolve this issue?

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

Answer: C

Explanation:

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

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

NEW QUESTION 162

- (Exam Topic 1)

A SysOps administrator is notified that an Amazon EC2 instance has stopped responding. The AWS Management Console indicates that the system status checks are failing. What should the administrator do first to resolve this issue?

- A. Reboot the EC2 instance so it can be launched on a new host.
- B. Stop and then start the EC2 instance so that it can be launched on a new host.
- C. Terminate the EC2 instance and relaunch it.
- D. View the AWS CloudTrail log to investigate what changed on the EC2 instance.

Answer: B

Explanation:

<https://aws.amazon.com/premiumsupport/knowledge-center/ec2-windows-system-status-check-fail/>

NEW QUESTION 163

- (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 168

- (Exam Topic 1)

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

How can this be accomplished?

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

Answer: B

NEW QUESTION 171

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

Answer: C

NEW QUESTION 173

- (Exam Topic 1)

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

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

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

Answer: C

NEW QUESTION 174

- (Exam Topic 1)

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

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

- A. Create a scheduled Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function to increase the desired capacity before peak times.
- B. Configure a scheduled scaling action with a recurrence option to change the desired capacity before and after peak times.
- C. Create a target tracking scaling policy to add more instances when memory utilization is above 70%.
- D. Configure the cooldown period for the Auto Scaling group to modify desired capacity before and after peak times.

Answer: B

Explanation:

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

NEW QUESTION 177

- (Exam Topic 2)

If your AWS Management Console browser does not show that you are logged in to an AWS account, close the browser and relaunch the console by using the AWS Management Console shortcut from the VM desktop.

If the copy-paste functionality is not working in your environment, refer to the instructions file on the VM desktop and use Ctrl+C, Ctrl+V or Command-C, Command-V.

Configure Amazon EventBridge to meet the following requirements.

- * 1. Use the us-east-2 Region for all resources,
- * 2. Unless specified below, use the default configuration settings.
- * 3. Use your own resource naming unless a resource name is specified below.
- * 4. Ensure all Amazon EC2 events in the default event bus are replayable for the past 90 days.
- * 5. Create a rule named RunFunction to send the exact message every 15 minutes to an existing AWS Lambda function named LogEventFunction.
- * 6. Create a rule named SpotWarning to send a notification to a new standard Amazon SNS topic named TopicEvents whenever an Amazon EC2 Spot Instance is interrupted. Do NOT create any topic subscriptions. The notification must match the following structure:

Input path:

```
{"instance": "$.detail.instance-id"}
```

Input Path:

```
{"instance": "$.detail.instance-id"}
```

Input template:

"The EC2 Spot Instance <instance> has been on account."

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Here are the steps to configure Amazon EventBridge to meet the above requirements:

- Log in to the AWS Management Console by using the AWS Management Console shortcut from the VM desktop. Make sure that you are logged in to the desired AWS account.
- Go to the EventBridge service in the us-east-2 Region.
- In the EventBridge service, navigate to the "Event buses" page.
- Click on the "Create event bus" button.
- Give a name to your event bus, and select "default" as the event source type.
- Navigate to "Rules" page and create a new rule named "RunFunction"
- In the "Event pattern" section, select "Schedule" as the event source and set the schedule to run every 15 minutes.
- In the "Actions" section, select "Send to Lambda" and choose the existing AWS Lambda function named "LogEventFunction"
- Create another rule named "SpotWarning"
- In the "Event pattern" section, select "EC2" as the event source, and filter the events on "EC2 Spot Instance interruption"
- In the "Actions" section, select "Send to SNS topic" and create a new standard Amazon SNS topic named "TopicEvents"
- In the "Input Transformer" section, set the Input Path to {"instance": "\$.detail.instance-id"} and Input template to "The EC2 Spot Instance <instance> has been interrupted on account."
- Now all Amazon EC2 events in the default event bus will be replayable for past 90 days. Note:
- You can use the AWS Management Console, AWS CLI, or SDKs to create and manage EventBridge resources.
- You can use CloudTrail event history to replay events from the past 90 days.
- You can refer to the AWS EventBridge documentation for more information on how to configure and use the service: <https://aws.amazon.com/eventbridge/>

NEW QUESTION 178

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

SOA-C02 Practice Exam Features:

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

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