Vendor: Amazon

Exam Code: SOA-C02

Exam Name: AWS Certified SysOps Administrator - Associate (SOA-C02)

Version: DEMO

QUESTION 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 very 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 po icy 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

QUESTION 2
An organization created an Amazon Elastic File System (Amazon EFS) volume with a file system ID of fs-85ba41fc, and it is actively used by 10 Amazon EC2 hosts.
The organization has become concerned that the file system is not encrypted.
How can this be resolved?

A. Enable encryption on each host's connection to the Amazon EFS volume.
   Each connection must be recreated for encryption to take effect.
B. Enable encryption on the existing EFS volume by using the AWS Command Line Interface.
C. Enable encryption on each host's local drive.
   Restart each host to encrypt the drive.
D. Enable encryption on a newly created volume and copy all data from the original volume.
   Reconnect each host to the new volume.

Answer: D
Explanation:
Amazon EFS supports two forms of encryption for file systems, encryption of data in transit and encryption at rest. You can enable encryption of data at rest when creating an Amazon EFS file system. You can enable encryption of data in transit when you mount the file system.
https://docs.aws.amazon.com/efs/latest/ug/encryption.html

QUESTION 3
Lab Simulation 3
You want to update an existing AWS CloudFormation stack. If needed, a copy of the CloudFormation template is available in an Amazon SB bucket named cloudformation-bucket

1. Use the us-east-2 Region for all resources.
2. Unless specified below, use the default configuration settings.

3. update the Amazon EQ instance named Devinstance by making the following changes to the stack named 1700182:

a) Change the EC2 instance type to us-east-t2.nano.
b) Allow SSH to connect to the EC2 instance from the IP address range 192.168.100.0/30.
c) Replace the instance profile IAM role with IamRoleB.

4. Deploy the changes by updating the stack using the CFServiceR01e role.
5. Edit the stack options to prevent accidental deletion.
6. Using the output from the stack, enter the value of the ProdInstanceId in the text box below:

[   ]

Answer:
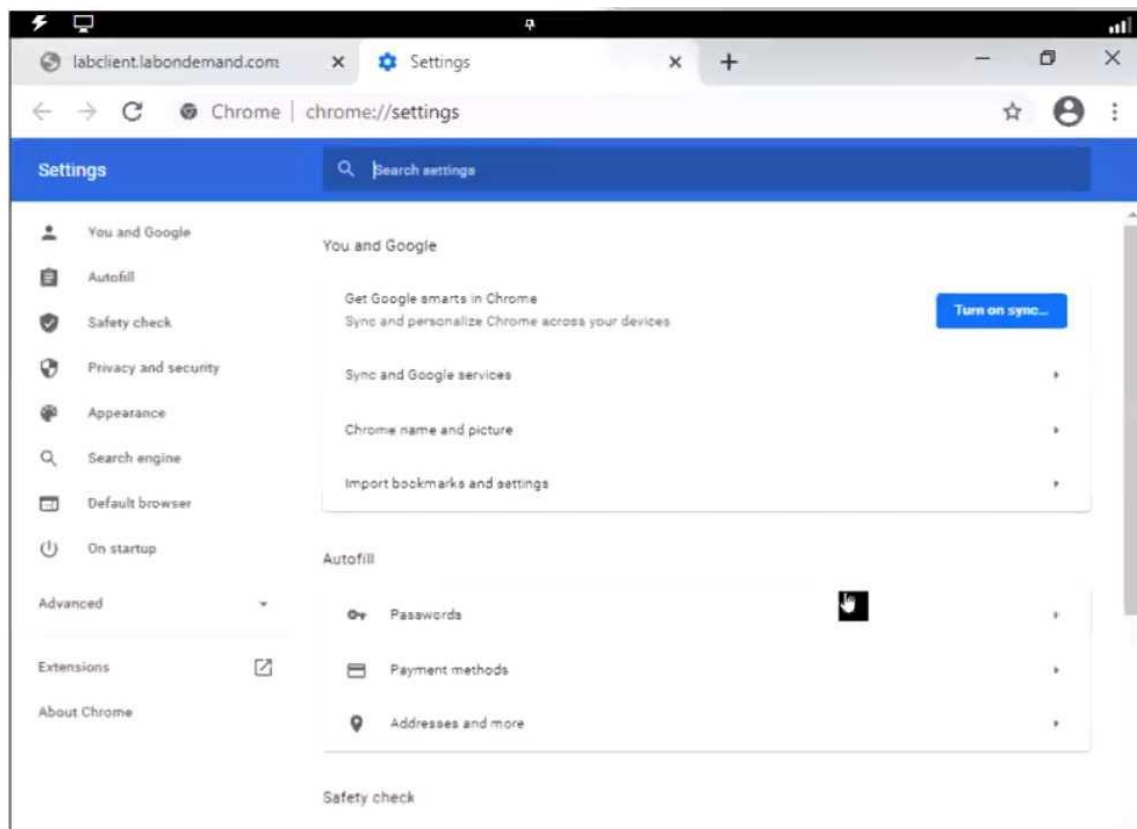
QUESTION 4
A company has multiple Amazon EC2 instances that run a resource-intensive application in a development environment.
A SysOps administrator is implementing a solution to stop these EC2 instances when they are not in use.
Which solution will meet this requirement?

A. Assess AWS CloudTrail logs to verify that there is no EC2 API activity.
    Invoke an AWS lambda function to stop the EC2 instances.
B. Create an Amazon CloudWatch alarm to stop the EC2 instances when the average CPU utilization is lower than 5% for a 30-minute period.

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

Answer: B
Explanation:
You can create an alarm that stops an Amazon EC2 instance when a certain threshold has been met.
You can create an alarm that is triggered when the average CPU utilization percentage has been lower than 10 percent for 24 hours, signaling that it is idle and no longer in use.
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/UsingAlarmActions.html#AddingStopActions

QUESTION 5
A company has an Amazon RDS DB instance.
The company wants to implement a caching service while maintaining high availability.
Which combination of actions will meet these requirements? (Choose two.)

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

Answer: CD
Explanation:
The main benefits of running your Amazon ElastiCache for Redis in Multi-AZ mode are enhanced availability and smaller need for administration.
https://aws.amazon.com/elasticache/faqs/?nc1=h_ls

QUESTION 6
A SysOps Administrator is running Amazon EC2 instances in multiple AWS Regions.
The Administrator wants to aggregate the CPU utilization for all instances onto an Amazon CloudWatch dashboard.
Each region should be present on the dashboard and represented by a single graph that contains the CPU utilization for all instances in that region.

How can the Administrator meet these requirements?

A. Create a cross-region dashboard using AWS Lambda and distribute it to all regions
B. Create a custom CloudWatch dashboard and add a widget for each region in the AWS Management Console
C. Enable cross-region dashboards under the CloudWatch section of the AWS Management Console
D. Switch from basic monitoring to detailed monitoring on all instances

Answer: C
Explanation:
Multi Region on a single Dashboard. Now cross accounts and cross region dashboards are supported. This is very new and maybe the question was before this new feature was introduced.
https://aws.amazon.com/blogs/aws/cross-account-cross-region-dashboards-with-amazon-

cloudwatch/

QUESTION 7
A company asks a SysOps administrator to ensure that AWS CloudTrail files are not tampered with after they are created.
Currently, the company uses AWS Identity and Access Management (IAM) to restrict access to specific trails.
The company's security team needs the ab lity to trace the integrity of each file.
What is the MOST operationally efficient solution that meets these requ rements?

A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function when a new file is delivered.
Configure the Lambda function to compute an MD5 hash check on the file and store the result in an Amazon DynamoDB table.
The security team can use the values that are stored in DynamoDB to verify the integrity of the delivered files.
B. Create an AWS Lambda function that is invoked each time a new file is delivered to the CloudTrail bucket.
Configure the Lambda function to compute an MD5 hash check on the file and store the result as a tag in an Amazon 53 object.
The security team can use the information in the tag to verify the integrity of the delivered files.
C. Enable the CloudTrail file integrity feature on an Amazon S3 bucket.
Create an IAM policy that grants the security team access to the file integrity logs that are stored in the S3 bucket.
D. Enable the CloudTrail file integrity feature on the trail.
The security team can use the digest file that is created by CloudTrail to verify the integrity of the delivered files.

Answer: D
Explanation:
When you enable log file integrity validation, CloudTrail creates a hash for every log file that it delivers. Every hour, CloudTrail also creates and delivers a file that references the log files for the last hour and contains a hash of each. This file is called a digest file. Validated log files are invaluable in security and forensic investigations
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html

QUESTION 8
An AWS CloudFormation template creates an Amazon RDS instance. This template is used to build up development environments as needed and then delete the stack when the environment is no longer required.
The RDS-persisted data must be retained for further use, even after the CloudFormation stack is deleted.

How can this be achieved in a reliable and efficient way?

A. Write a script to continue backing up the RDS instance every five minutes
B. Create an AWS Lambda function to take a snapshot of the RDS instance, and manually execute the function before deleting the stack
C. Use the Snapshot Deletion Policy in the CloudFormation template definition of the RDS instance
D. Create a new CloudFormation template to perform backups of the RDS instance, and run this template before deleting the stack

Answer: C

Explanation:
With the DeletionPolicy attribute you can preserve or (in some cases) backup a resource when its stack is deleted. You specify a DeletionPolicy attribute for each resource that you want to control. If a resource has no DeletionPolicy attribute, AWS CloudFormation deletes the resource by default.

QUESTION 9
A SysOps administrator is responsible for the administration of an online application that utilizes an Amazon CloudFront web distribution, an Application Load Balancer (ALB), Amazon RDS, and Amazon EC2 inside a VPC. All services are logged. The administrator must conduct an investigation into the HTTP Layer 7 status codes returned by the web application.

Where are the status codes stored in the log files? (Select two.)

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

Answer: CD
Explanation:
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
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

QUESTION 10
A data analytics application is running on an Amazon EC2 instance. A SysOps administrator must add custom dimensions to the metrics collected by the Amazon CloudWatch agent.
How can the SysOps administrator meet this requirement?

A. Create a custom shell script to extract the dimensions and collect the metrics using the Amazon CloudWatch agent.
B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to evaluate the required custom dimensions and send the metrics to Amazon Simple Notification Service (Amazon SNS).
C. Create an AWS Lambda function to collect the metrics from AWS CloudTrail and send the metrics to an Amazon CloudWatch Logs group.
D. Create an append_dimensions field in the Amazon CloudWatch agent configuration file to collect the metrics.

Answer: D
Explanation:
In custom metrics, the --dimensions parameter is common. A dimension further clarifies what the metric is and what data it stores. You can have up to 30 dimensions assigned to one metric, and each dimension is defined by a name and value pair.
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/publishingMetrics.html

QUESTION 11
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 Rekognition.
C. Enable Amazon GuardDuty. Configure S3 protection to monitor all data inside Amazon S3.
D. Enable Amazon Macie. Create a discovery job that uses the managed data identifier.

Answer: D
Explanation:
To discover sensitive data with Amazon Macie, you create and run sensitive data discovery jobs.
A sensitive data discovery job analyzes objects in Amazon Simple Storage Service (Amazon S3) buckets to determine whether the objects contain sensitive data, and it provides detailed reports of the sensitive data that it finds and the analysis that it performs. By creating and running jobs, you can automate discovery, logging, and reporting of sensitive data in S3 buckets.
https://docs.aws.amazon.com/macie/latest/user/data-classification.html

QUESTION 12
A SysOps administrator is attempting to deploy resources by using an AWS CloudFormation template. An Amazon EC2 instance that is defined in the template fails to launch and produces an InsufficientInstanceCapacity error.
Which actions should the SysOps administrator take to resolve this error? (Choose two.)

A. Create a separate AWS CloudFormation template for the EC2 instance.
B. Modify the AWS CloudFormation template to not specify an Availability Zone for the EC2 instance.
C. Modify the AWS CloudFormation template to use a different EC2 instance type.
D. Use a different Amazon Machine Image (AMI) for the EC2 instance.
E. Use the AWS CLI's validate-template command before creating a stack from the template.

Answer: BC
Explanation:
If you're launching an instance, submit a new request without specifying an Availability Zone.
If you're launching an instance, submit a new request using a different instance type (which you can resize at a later stage). For more information, see Change the instance type.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/troubleshooting-
launch.html#troubleshooting-launch-capacity

QUESTION 13
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
Explanation:
Target.FailedHealthChecks
Verify that the target is listening for traffic on the health check port. You can use the ss command on Linux targets to verify which ports your server is listening on. For Windows targets, you can use the netstat command.
https://aws.amazon.com/premiumsupport/knowledge-center/elb-fix-failing-health-checks-alb/

QUESTION 14
A SysOps administrator has created an AWS Service Catalog portfolio and has shared the portfolio with a second AWS account in the company. The second account is controlled by a different administrator.
Which action will the administrator of the second account be able to perform?

A. Add a product from the imported portfolio to a local portfolio.
B. Add new products to the imported portfolio.
C. Change the launch role for the products contained in the imported portfolio.
D. Customize the products in the imported portfolio.

Answer: A
Explanation:
When you share a portfolio using account-to-account sharing or AWS Organizations, you allow an AWS Service Catalog administrator of another AWS account to import your portfolio into his or her account and distribute the products to end users in that account.
https://docs.aws.amazon.com/servicecatalog/latest/adminguide/catalogs_portfolios_sharing.html

QUESTION 15
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. Replace the original volume with a volume that is created from the snapshot.

Answer: A
Explanation:
After you increase the size of an EBS volume, use the Windows Disk Management utility or PowerShell to extend the disk size to the new size of the volume. You can begin resizing the file system as soon as the volume enters the optimizing state.
https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/recognize-expanded-volume-windows.html

QUESTION 16
A SysOps administrator is using Amazon EC2 instances to host an application. The SysOps

administrator needs to grant permissions for the application to access an Amazon DynamoDB table.
Which solution will meet this requirement?

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

Answer: D
Explanation:
Access to Amazon DynamoDB requires credentials. Those credentials must have permissions to access AWS resources, such as an Amazon DynamoDB table or an Amazon Elastic Compute Cloud (Amazon EC2) instance. The following sections provide details on how you can use AWS Identity and Access Management (IAM) and DynamoDB to help secure access to your resources. https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/authentication-and-access-control.html

QUESTION 17
A SysOps administrator must configure Amazon S3 to host a simple nonproduction webpage.
The SysOps administrator has created an empty S3 bucket from the AWS Management Console.
The S3 bucket has the default configuration in place.
Which combination of actions should the SysOps administrator take to complete this process?
(Choose two.)

A. Configure the S3 bucket by using the "Redirect requests for an object" functionality to point to the bucket root URL.
B. Turn off the "Block all public access" setting.
    Allow public access by using a bucket ACL that contains <Permission>WEBSITE</Permission>.
C. Turn off the "Block all public access" setting.
    Allow public access by using a bucket ACL that allows access to the AuthenticatedUsers grantee.
D. Turn off the "Block all public access" setting.
    Set a bucket policy that allows "Principal": the s3:GetObject action.
E. Create an index.html document.
    Configure static website hosting, and upload the index document to the S3 bucket.

Answer: DE
Explanation:
Step 1: Create a bucket
Step 2: Enable static website hosting
Step 3: Edit Block Public Access settings
Step 4: Add a bucket policy that makes your bucket content publicly available
Step 5: Configure an index document
Step 6: Configure an error document
Step 7: Test your website endpoint
Step 8: Clean up
https://docs.aws.amazon.com/AmazonS3/latest/userguide/HostingWebsiteOnS3Setup.html

QUESTION 18
A SysOps administrator is responsible for managing a company's cloud infrastructure with AWS CloudFormation. The SysOps administrator needs to create a single resource that consists of multiple AWS services. The resource must support creation and deletion through the CloudFormation console.
Which CloudFormation resource type should the SysOps administrator create to meet these requirements?

A.   AWS::EC2::Instance with a cfn-init helper script
B.   AWS::OpsWorks::Instance
C.   AWS::SSM::Document
D.   Custom::MyCustomType

Answer: D
Explanation:
Custom resources enable you to write custom provisioning logic in templates that AWS CloudFormation runs anytime you create, update (if you changed the custom resource), or delete stacks. For example, you might want to include resources that aren't available as AWS CloudFormation resource types. You can include those resources by using custom resources. That way you can still manage all your related resources in a single stack.
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/template-custom-resources.html

QUESTION 19
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 tor 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
Explanation:
Amazon S3 is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Amazon S3. CloudTrail captures a subset of API calls for Amazon S3 as events, including calls from the Amazon S3 console and code calls to the Amazon S3 APIs.
https://docs.aws.amazon.com/AmazonS3/latest/userguide/cloudtrail-logging.html

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: ASTR14