

➤ **Vendor: Amazon**

➤ **Exam Code: SOA-C02**

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

➤ **New Updated Questions from [Braindump2go](https://www.braindump2go.com)**

➤ **(Updated in [November/2022](#))**

Visit Braindump2go and Download Full Version SOA-C02 Exam Dumps

QUESTION 322

A company is creating a new multi-account architecture. A Sysops administrator must implement a login solution to centrally manage user access and permissions across all AWS accounts. The solution must be integrated with AWS Organizations and must be connected to a third-party Security Assertion Markup Language (SAML) 2.0 identity provider (IdP).

What should the SysOps administrator do to meet these requirements?

- A. Configure an Amazon Cognito user pool. Integrate the user pool with the third-party IdP.
- B. Enable and configure AWS Single Sign-On with the third-party IdP.
- C. Federate the third-party IdP with AWS Identity and Access Management (IAM) for each AWS account in the organization.
- D. Integrate the third-party IdP directly with AWS Organizations.

Answer: A

QUESTION 323

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

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

- A. Create and attach a NAT gateway.
Create a custom route table that includes an entry to point all IPv6 traffic to the NAT gateway.
Attach the custom route table to the IPv6-only subnets.
- B. Create and attach an internet gateway.
Create a custom route table that includes an entry to point all IPv6 traffic to the internet gateway.
Attach the custom route table to the IPv6-only subnets.
- C. Create and attach an egress-only internet gateway.
Create a custom route table that includes an entry to point all IPv6 traffic to the egress-only internet gateway.
Attach the custom route table to the IPv6-only subnets.
- D. Create and attach an internet gateway and a NAT gateway.
Create a custom route table that includes an entry to point all IPv6 traffic to the internet gateway and all IPv4 traffic to the NAT gateway. Attach the custom route table to the IPv6-only subnets.

Answer: C

QUESTION 324

A company wants to track its AWS costs in all member accounts that are part of an organization in AWS Organizations.

[SOA-C02 Exam Dumps](#) [SOA-C02 Exam Questions](#) [SOA-C02 PDF Dumps](#) [SOA-C02 VCE Dumps](#)

<https://www.braindump2go.com/soa-c02.html>

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

QUESTION 325

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

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

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

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

Answer: A

QUESTION 326

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

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

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

Answer: C

QUESTION 327

A company plans to migrate several of its high performance computing (HPC) virtual machines (VMs) to Amazon EC2 instances on AWS.

A SysOps administrator must identify a placement group for this deployment.

The strategy must minimize network latency and must maximize network throughput between the HPC VMs.

Which strategy should the SysOps administrator choose to meet these requirements?

- A. Deploy the instances in a cluster placement group in one Availability Zone.

- B. Deploy the instances in a partition placement group in two Availability Zones.
- C. Deploy the instances in a partition placement group in one Availability Zone.
- D. Deploy the instances in a spread placement group in two Availability Zones.

Answer: A

QUESTION 328

A company's VPC has connectivity to an on-premises data center through an AWS Site-to-Site VPN. The company needs Amazon EC2 instances in the VPC to send DNS queries for example.com to the DNS servers in the data center.

Which solution will meet these requirements?

- A. Create an Amazon Route 53 Resolver inbound endpoint.
Create a conditional forwarding rule on the on-premises DNS servers to forward DNS requests for example.com to the inbound endpoints.
- B. Create an Amazon Route 53 Resolver inbound endpoint.
Create a forwarding rule on the resolver that sends all queries for example.com to the on-premises DNS servers.
Associate this rule with the VPC.
- C. Create an Amazon Route 53 Resolver outbound endpoint.
Create a conditional forwarding rule on the on-premises DNS servers to forward DNS requests for example.com to the outbound endpoints.
- D. Create an Amazon Route 53 Resolver outbound endpoint.
Create a forwarding rule on the resolver that sends all queries for example.com to the on-premises DNS servers.
Associate this rule with the VPC.

Answer: C

QUESTION 329

A software company runs a workload on Amazon EC2 instances behind an Application Load Balancer (ALB). A SysOps administrator needs to define a custom health check for the EC2 instances. What is the MOST operationally efficient solution?

- A. Set up each EC2 Instance so that it writes its healthy/unhealthy status into a shared Amazon S3 bucket for the ALB to read
- B. Configure the health check on the ALB and ensure that the HealthCheckPath setting is correct
- C. Set up Amazon ElastiCache to track the EC2 instances as they scale in and out
- D. Configure an Amazon API Gateway health check to ensure custom checks on all of the EC2 instances

Answer: B

QUESTION 330

A SysOps administrator is tasked with analyzing database performance. The database runs on a single Amazon RDS D6 instance. The SysOps administrator finds that, during times of peak traffic, resources on the database are overutilized due to the amount of read traffic.

Which actions should the SysOps administrator take to improve RDS performance? (Select TWO.)

- A. Add a read replica.
- B. Modify the application to use Amazon ElastiCache for Memcached.
- C. Migrate the database from RDS to Amazon DynamoDB.
- D. Migrate the database to Amazon EC2 with enhanced networking enabled
- E. Upgrade the database to a Multi-AZ deployment.

Answer: AB

QUESTION 331

A company recently migrated 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 CloudWatch.
AWS automatically installs and configures the agents for the specified instances.
- B. Install and configure the CloudWatch agent on all the instances.
Attach an IAM role to allow the instances to write logs to CloudWatch.
- C. Install and configure the CloudWatch agent on all the instances.
Attach an IAM user to allow the instances to write logs to CloudWatch.
- D. Install and configure the CloudWatch agent on all the instances.
Attach the necessary security groups to allow the instances to write logs to CloudWatch.

Answer: C

QUESTION 332

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 as 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

QUESTION 333

A company applies user-defined tags to resources that are associated with the company's AWS workloads. Twenty days after applying the tags, the company notices that it cannot use the tags to filter views in the AWS Cost Explorer console.

What is the reason for this issue?

- A. It takes at least 30 days to be able to use tags to filter views in Cost Explorer.
- B. The company has not activated the user-defined tags for cost allocation.
- C. The company has not created an AWS Cost and Usage Report.
- D. The company has not created a usage budget in AWS Budgets.

Answer: B

QUESTION 334

A company's SysOps administrator must ensure that all Amazon EC2 Windows instances that are launched in an AWS account have a third-party agent installed. The third-party agent has an MSI package. The company uses AWS Systems Manager for patching, and the Windows instances are tagged appropriately. The third-party agent requires periodic updates as new versions are released. The SysOps administrator must deploy these updates automatically. Which combination of steps will meet these requirements with the LEAST operational effort? (Select TWO.)

- A. Create a Systems Manager Distributor package for the third-party agent.
Make sure that Systems Manager Inventory is configured.
If Systems Manager Inventory is not configured, set up a new inventory for instances that is based on the appropriate tag value for Windows.
- B. Create a Systems Manager State Manager association to run the AWS-RunRemoteScript

document.

Populate the details of the third-party agent package.

Specify instance tags based on the appropriate tag value for Windows with a schedule of 1 day.

- C. Create a Systems Manager State Manager- association to run the AWS-ConfigureAWSPackage document.

Populate the details of the third-party agent package.

Specify instance tags based on the appropriate tag value for Windows with a schedule of 1 day.

- D. Create a Systems Manager Opsitem with the tag value for Windows.
Attach the Systems Manager Distributor package to the Opsitem.
Create a maintenance window that is specific to the package deployment.
Configure the maintenance window to cover 24 hours a day.

Answer: D

QUESTION 335

A global gaming company is preparing to launch a new game on AWS. The game runs in multiple AWS Regions on a fleet of Amazon EC2 instances. The instances are in an Auto Scaling group behind an Application Load Balancer (ALB) in each Region. The company plans to use Amazon Route 53 for DNS services. The DNS configuration must direct users to the Region that is closest to them and must provide automated failover.

Which combination of steps should a SysOps administrator take to configure Route 53 to meet these requirements? (Select TWO.)

- A. Create Amazon CloudWatch alarms that monitor the health of the ALB in each Region.
Configure Route 53 DNS failover by using a health check that monitors the alarms.
- B. Create Amazon CloudWatch alarms that monitor the health of the EC2 instances in each Region.
Configure Route 53 DNS failover by using a health check that monitors the alarms.
- C. Configure Route 53 DNS failover by using a health check that monitors the private address of an EC2 instance in each Region.
- D. Configure Route 53 geoproximity routing Specify the Regions that are used for the infrastructure.
- E. Configure Route 53 simple routing Specify the continent, country, and state or province that are used for the infrastructure.

Answer: A

QUESTION 336

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

QUESTION 337

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 with 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

QUESTION 338

A company maintains a large set of sensitive data in an Amazon S3 bucket.

The company's security team asks a SysOps administrator to help verify that all current objects in the S3 bucket are encrypted.

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

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

Answer: B

QUESTION 339

A company has a high-performance Windows workload. The workload requires a storage volume that provides consistent performance of 10,000 Kbps. The company does not want to pay for additional unneeded capacity to achieve this performance.

Which solution will meet these requirements with the LEAST cost?

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

Answer: A

QUESTION 340

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.
In the route table for the private subnets, add a route to the NAT gateway.
- C. Add a NAT gateway to a public subnet in the route table for the private subnets, add a route to the NAT gateway.
- D. Add two internet gateways to the VPC.
In the route table for the private subnets and public subnets, add a route to each internet gateway.

Answer: C

QUESTION 341

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.

[SOA-C02 Exam Dumps](#) [SOA-C02 Exam Questions](#) [SOA-C02 PDF Dumps](#) [SOA-C02 VCE Dumps](#)

<https://www.braindump2go.com/soa-c02.html>

(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

QUESTION 342

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

QUESTION 343

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

QUESTION 344

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

QUESTION 345

[SOA-C02 Exam Dumps](#) [SOA-C02 Exam Questions](#) [SOA-C02 PDF Dumps](#) [SOA-C02 VCE Dumps](#)

<https://www.braindump2go.com/soa-c02.html>

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

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

Answer: A

QUESTION 346

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

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

Answer: D

QUESTION 347

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: D

QUESTION 348

A company uses Amazon S3 to aggregate raw video footage from various media teams across the US. The company recently expanded into new geographies in Europe and Australia. The technical teams located in Europe and Australia reported delays when uploading large video files into the destination S3 bucket in the United States. What are the MOST cost-effective ways to increase upload speeds into the S3 bucket? (Select TWO.)

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

Answer: CE

[SOA-C02 Exam Dumps](#) [SOA-C02 Exam Questions](#) [SOA-C02 PDF Dumps](#) [SOA-C02 VCE Dumps](#)

<https://www.braindump2go.com/soa-c02.html>

QUESTION 349

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 incur additional compute, storage, or database costs. Which solution will meet these requirements?

- A. Configure AWS Cost and Usage Reports to send a daily report to an Amazon S3 bucket. Create an AWS Lambda function that will evaluate. Spend by service and notify each team by using Amazon Simple Notification Service (Amazon SNS) notifications. Invoke the Lambda function when a report is placed in the S3 bucket.
- B. Configure AWS Cost and Usage Reports to send a daily report to an Amazon S3 bucket. 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.
- C. 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.
- D. Use AWS Budgets to create a cost budget for each team, filtering by the services they own. 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

QUESTION 350

A company plans to launch a static website on its domain example.com and subdomain www.example.com using Amazon S3. How should the SysOps administrator meet this requirement?

- A. Create one S3 bucket named example.com for both the domain and subdomain.
- B. Create one S3 bucket with a wildcard named *.example.com for both the domain and subdomain.
- C. Create two S3 buckets named example.com and www.example.com. Configure the subdomain bucket to redirect requests to the domain bucket.
- D. Create two S3 buckets named http://www.example.com and http://example.com. Configure the wildcard (*) bucket to redirect requests to the domain bucket.

Answer: C

QUESTION 351

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

QUESTION 352

A SysOps administrator has blocked public access to all company Amazon S3 buckets. The SysOps administrator

[SOA-C02 Exam Dumps](#) [SOA-C02 Exam Questions](#) [SOA-C02 PDF Dumps](#) [SOA-C02 VCE Dumps](#)

<https://www.braindump2go.com/soa-c02.html>

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.
Set up Amazon Simple Notification Service (Amazon SNS) to send notifications
- C. Enable S3 Event notifications for each S3 bucket.
Subscribe S3 Event Notifications to an Amazon Simple Notification Service (Amazon SNS) topic.
- D. Enable the s3-bucket-public-read-prohibited managed rule in AWS Config.
Subscribe the AWS Config rule to an Amazon Simple Notification Service (Amazon SNS) topic.

Answer: D

QUESTION 353

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

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

Answer: A

QUESTION 354

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

QUESTION 355

Lab Simulation 1

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.

[SOA-C02 Exam Dumps](#) [SOA-C02 Exam Questions](#) [SOA-C02 PDF Dumps](#) [SOA-C02 VCE Dumps](#)

<https://www.braindump2go.com/soa-c02.html>

Configure Amazon EventBridge to meet the following requirements.

1. use the us-east-2LRegion 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 template:

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

Answer:



Event pattern Info

☒ Event pattern form ☐ Custom patterns (JSON editor)

Event source
AWS service or EventBridge partner as source

AWS services

AWS service
The name of the AWS service as the event source

EC2

Event type
The type of events as the source of the matching pattern

EC2 Spot Instance Interruption Warning

Event pattern
Event pattern, or filter to match the events

```
{
  "source": ["aws.ec2"],
  "detail-type": ["EC2 Spot Instance Interruption Warning"]
}
```

Copy Test pattern Edit pattern

Cancel Previous Next

Target 1

Target types
Select an EventBridge event bus, EventBridge API destination (AWS partner), or another AWS service as a target.

☐ EventBridge event bus
☐ EventBridge API destination
☒ AWS service

Select a target [Info](#)
Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule)

Select target type ▼

Add another target

Cancel Previous **Next**

Event pattern [Info](#)

☒ Event pattern form ☐ Custom patterns (JSON editor)

Event pattern
Enter an event pattern in JSON. You can test the event pattern against the sample event. You can also go to the defined pattern.

Select matching pattern ▼ ☐ Content-based filter syntax

```
1 {  
2   "source": ["aws:ec2"],  
3   "detail-type": ["EC2 Spot Instance Interruption Warning"]  
4 }
```

JSON is valid

Step 1: Create rule

Create rules to invoke Targets based on Events happening in your AWS environment.

Event Source

Build or customize an Event Pattern or set a Schedule to invoke Targets.

☒ Event Pattern  ☐ Schedule 

Build event pattern to match events by service

Service Name

Event Type

▼ Event Pattern Preview

[Copy to clipboard](#) [Edit](#)

```
{
  "source": [
    "aws.ec2"
  ],
  "detail-type": [
    "EC2 Spot Instance Interruption Warning"
  ]
}
```





► Show sample event(s)

Targets

Select Target to invoke when an event matches your Event Pattern or when schedule is triggered.

Topic*

▼ Configure input

- ☐ Matched event 
☐ Part of the matched event 
☐ Constant (JSON text) 
☒ Input Transformer 

Input Template: A string containing placeholders which will be filled with

 Add target*

* Required

[Cancel](#)

[Configure details](#)

Step 2: Configure rule details

Rule definition

Name*

Description

State ☒ Enabled

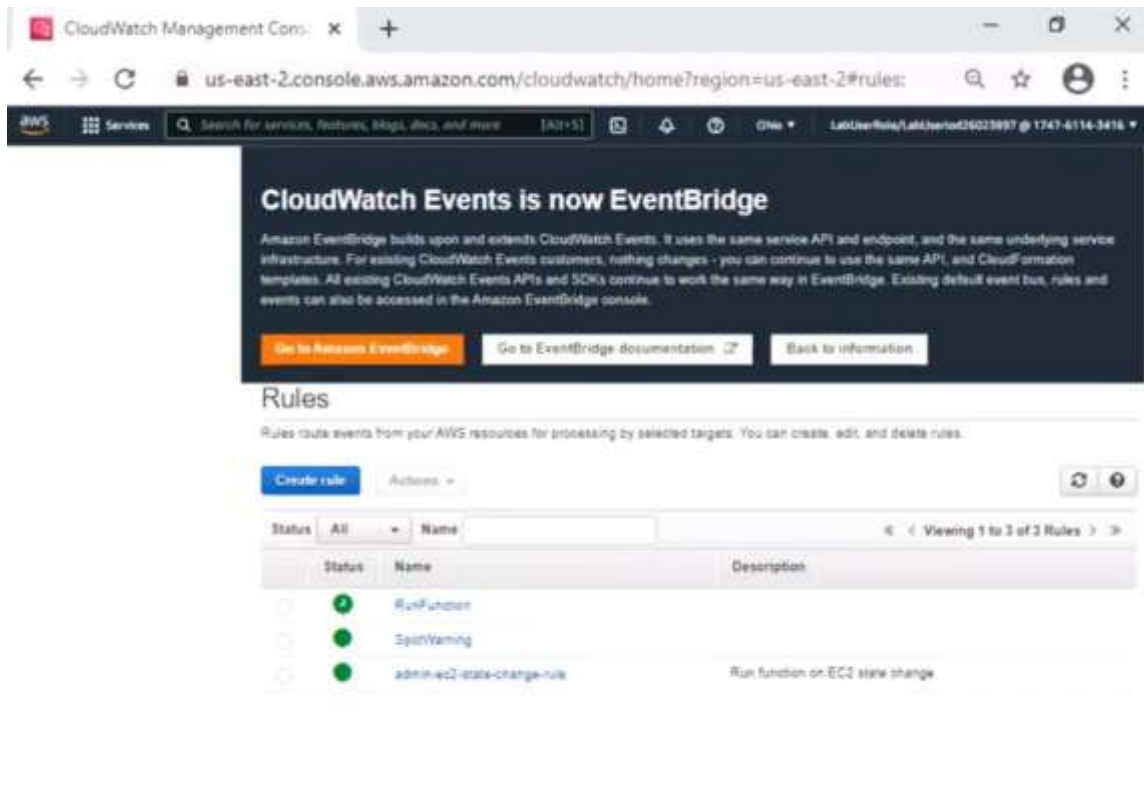
CloudWatch Events will add necessary permissions for target(s) so they can be invoked when this rule is triggered.

* Required

[Cancel](#)

[Back](#)

[Create rule](#)



CloudWatch Events is now EventBridge

Amazon EventBridge builds upon and extends CloudWatch Events. It uses the same service API and endpoint, and the same underlying service infrastructure. For existing CloudWatch Events customers, nothing changes - you can continue to use the same API, and CloudFormation templates. All existing CloudWatch Events APIs and SDKs continue to work the same way in EventBridge. Existing default event bus, rules and events can also be accessed in the Amazon EventBridge console.

[Go to Amazon EventBridge](#) [Go to EventBridge documentation](#) [Back to information](#)

Rules

Rules route events from your AWS resources for processing by selected targets. You can create, edit, and delete rules.

[Create rule](#) [Actions](#)

Status: **All** Name: < Viewing 1 to 3 of 3 Rules >

Status	Name	Description
<input checked="" type="radio"/>	RunFunction	
<input checked="" type="radio"/>	SpinVaming	
<input checked="" type="radio"/>	admin-ec2-state-change-rule	Run function on EC2 state change