SOA-C02 Q&As

AWS Certified SysOps Administrator - Associate (SOA-C02)

Pass Amazon SOA-C02 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/soa-c02.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon Official Exam Center

QUESTION 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 instances. Instruct the team to use AWS Systems Manager Session Manager to connect to the Instances by using the assumed IAM role.

B. Associate an Elastic IP address and a security group with each instance. Add the engineers\\' IP addresses to the security group inbound rules. Add a statement to the IAM role policy to allow the ec2:AuthoflzeSecurityGroupIngress action so that the team can connect to the Instances.

C. Create a bastion host with an EC2 Instance, and associate the bastion host with the VPC. Add a statement to the IAM role policy to allow the ec2:CreateVpnConnection action on the bastion host. Instruct the team to use the bastion host endpoint to connect to the instances.

D. Create an internet-facing Network Load Balancer. Use two listeners. Forward port 22 to a target group of Linux instances. Forward port 3389 to a target group of Windows Instances. Add a statement to the IAM role policy to allow the ec2:CreateRoute action so that the team can connect to the Instances.

Correct Answer: A

https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html

QUESTION 2

A SysOps administrator is configuring Amazon CloudWatch alarms. A particular is constantly in the ALARM state. What could be the reason for this issue?

A. Alarms continue to evaluate metrics against configured thresholds, even after they are triggered.

B. After alarms are triggered, they remain in the ALARM state until they are manually disabled.

C. After an alarm is triggered and an action is performed, the application logic must reset the alarm to its normal state.

D. The alarm is not receiving appropriate metrics.

Correct Answer: A

For any period of one minute or longer, an alarm is evaluated every minute and the evaluation is based on the window of time defined by the Period and Evaluation Periods. For example, if the Period is 5 minutes (300 seconds) and Evaluation Periods is 1, then at the end of minute 5 the alarm evaluates based on data from minutes 1 to 5. Then at the end of minute 6, the alarm is evaluated based on the data from minutes 2 to 6.

QUESTION 3

CORRECT TEXT

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-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 1 5 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:

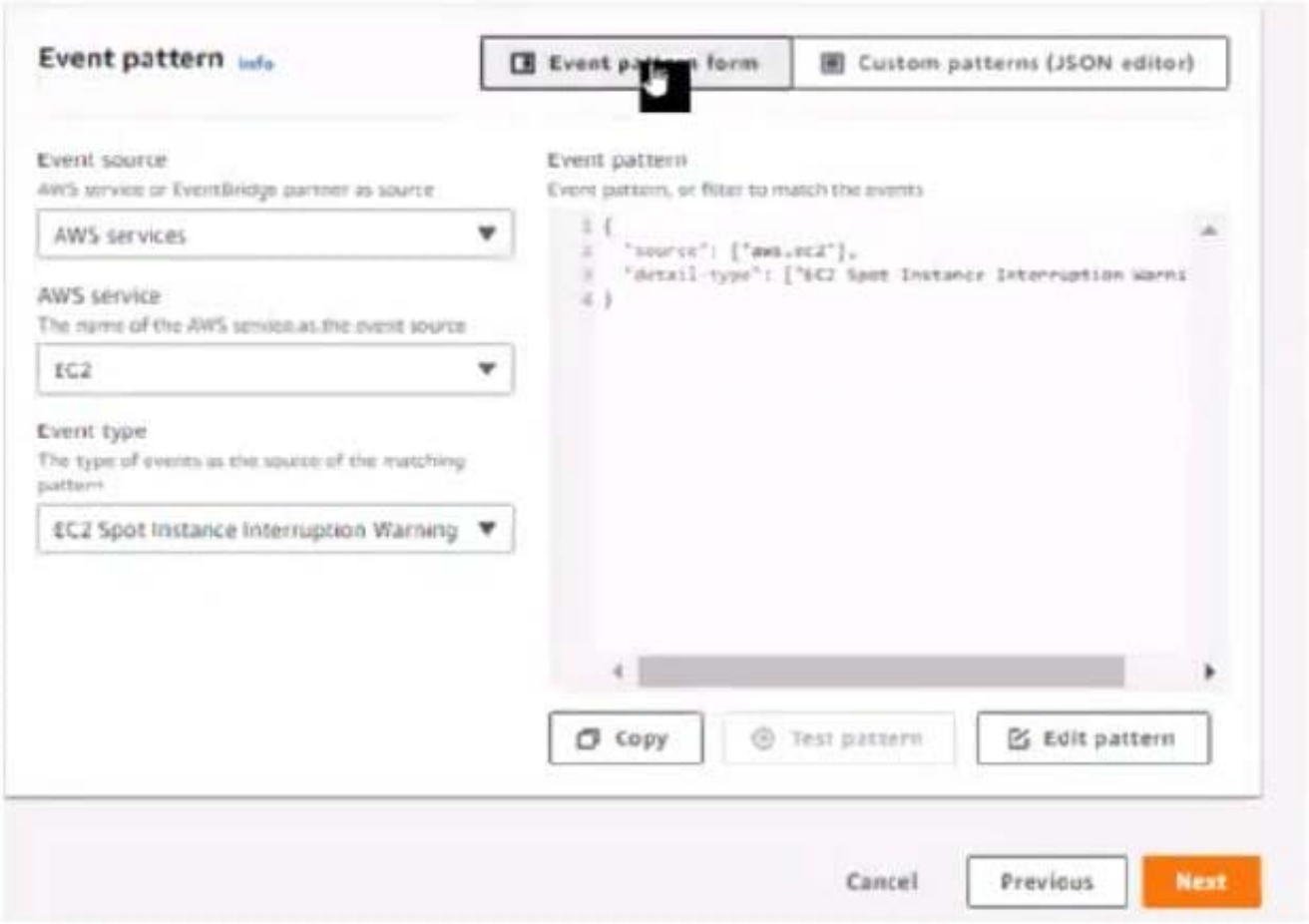
```
{"instance":"$.detail.instance-id"}
```

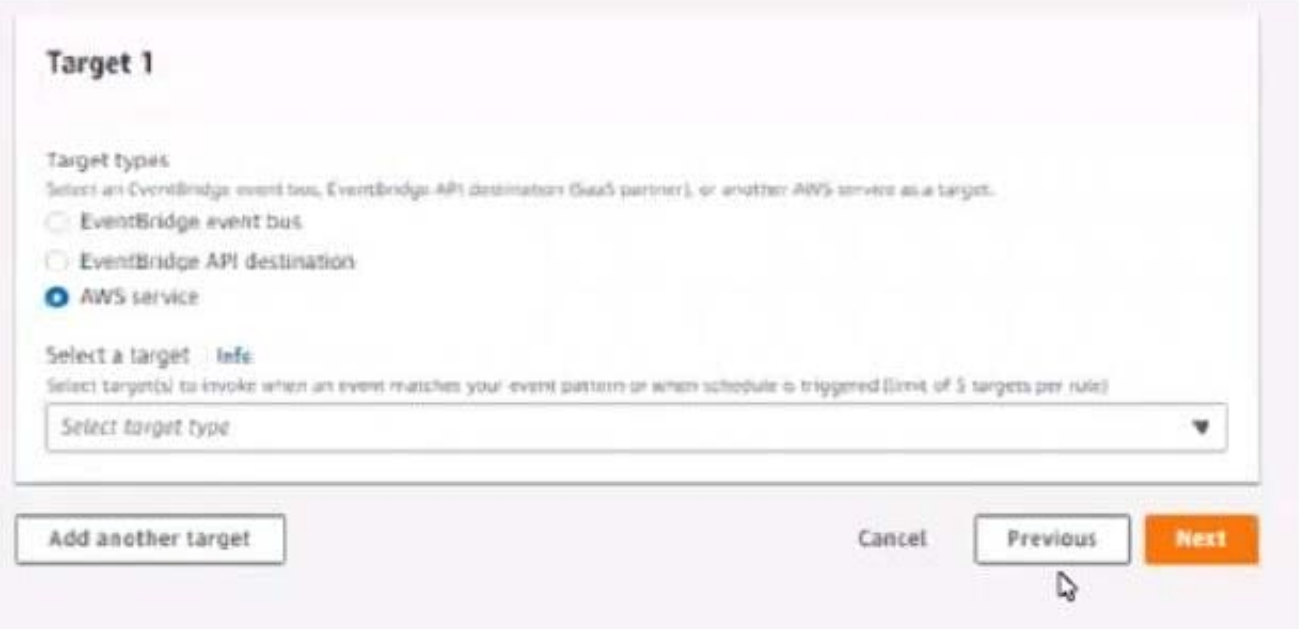
Input template:

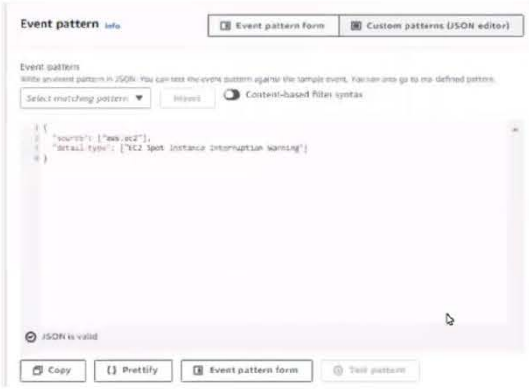
" The EC2 Spot Instance has been on account.

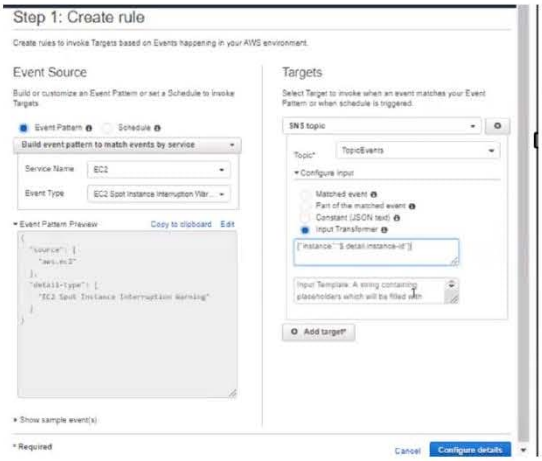
Correct Answer: Check the answer in explanation.

Solution as given below.

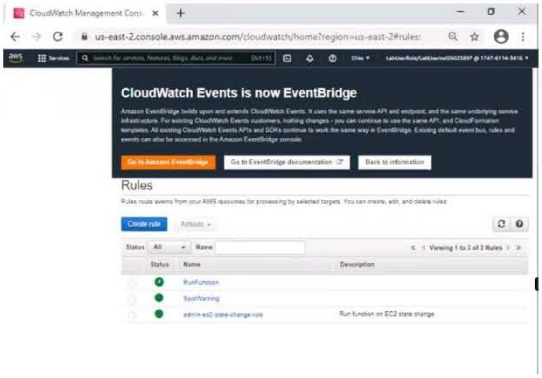

Event pattern info
Event pattern form
Custom patterns (JSON editor)
Event source
AWS service or EventBridge partner as source
AWS services
AWS service
The name of the AWS service as the event source
EC2
Event type
The type of events as the source of the matching pattern
EC2 Spot Instance Interruption Warning
Event pattern
Event pattern, or filter to match the events
{
"source": ["aws.ec2"],
"detail-type": ["EC2 Spot Instance Interruption Warni
}
Copy
Test pattern
Edit pattern
Cancel
Previous
Next


Target 1
Target types
EventBridge event bus
EventBridge API destination
AWS service
Select a target info
Select target type
Add another target
Cancel
Previous
Next


Event pattern
Event pattern form
Custom patterns (JSON editor)
Event pattern
Content-based filter syntax
JSON is valid
Copy
Prettify
Event pattern form


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
EC2
Event Type
EC2 Spot Instance Interruption War...
Event Pattern Preview
Copy to clipboard
Edit
Targets
Select Target to invoke when an event matches your Event Pattern or when schedule is triggered.
SNS topic
Topic*
TopicEvents
Configure input
Matched event
Part of the matched event
Constant (JSON text)
Input Transformer
Add target*
Show sample event(s)
* 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 Management Cons
us-east-2.console.aws.amazon.com/cloudwatch/home?region=us-east-2#rules:
CloudWatch Events is now EventBridge
Go to Amazon EventBridge
Go to EventBridge documentation
Back to information
Rules
Create rule
Actions
Status
All
Name
Viewing 1 to 3 of 3 Rules
Status
Name
Description
RunFunction
SpotWarning
Run function on EC2 state change

QUESTION 4

A company needs to deploy a new workload on AWS. The company must encrypt all data at rest and must rotate the encryption keys once each year. The workload uses an Amazon RDS for MySQL Multi-AZ database for data storage. Which configuration approach will meet these requirements?

A. Enable Transparent Data Encryption (TDE) in the MySQL configuration file. Manually rotate the key every 12 months.

B. Enable RDS encryption on the database at creation time by using the AWS managed key for Amazon RDS.

C. Create a new AWS Key Management Service (AWS KMS) customer managed key. Enable automatic key rotation. Enable RDS encryption on the database at creation time by using the KMS key.

D. Create a new AWS Key Management Service (AWS KMS) customer managed key. Enable automatic key rotation. Enable encryption on the Amazon Elastic Block Store (Amazon EBS) volumes that are attached to the RDS DB instance.

Correct Answer: C

This configuration approach will meet the requirement of encrypting all data at rest and rotating the encryption keys once each year. By creating a new AWS KMS customer managed key and enabling automatic key rotation, the encryption keys will be rotated automatically every year. By enabling RDS encryption on the database at creation time using the KMS key, all data stored in the RDS for MySQL Multi-AZ database will be encrypted at rest. This approach provide more control over key management and rotation and provide additional security benefits.

QUESTION 5

A company\\'s SysOps administrator deploys a public Network Load Balancer (NLB) in front of the company\\'s web application. The web application does not use any Elastic IP addresses. Users must access the web application by using the company\\'s domain name. The SysOps administrator needs to configure Amazon Route 53 to route traffic to the NLB. Which solution will meet these requirements MOST cost-effectively?

A. Create a Route 53 AAAA record for the NLB.

B. Create a Route 53 alias record for the NLB.

C. Create a Route 53 CAA record for the NLB.

D. Create a Route 53 CNAME record for the NLB.

Correct Answer: B

A record = URL to IPv4 AAAA record = URL to IPv6 CNAME record = URL to URL (All the same, one url = Many URL\\'s) Alias record = AWS service