



## Download Free Amazon SOA-C02 Exam PDF | PrepBolt

Don't miss out! Download the latest free Amazon AWS Certified SysOps Administrator - Associate exam PDF questions. Access real SOA-C02 dumps with verified answers and boost your chances to pass your certification on the first try with [PrepBolt](https://prepbolt.com/SOA-C02.html) SOA-C02 exam pdf questions and answers.

Thank you for Downloading SOA-C02 exam PDF Demo

<https://prepbolt.com/SOA-C02.html>

QUESTIONS & ANSWERS  
**DEMO VERSION**  
*(LIMITED CONTENT)*

# Question 1

---

Question Type: MultipleChoice

---

[Security and Compliance]

A company has an AWS Config rule that identifies open SSH ports in security groups. The rule has an automatic remediation action to delete the SSH inbound rule for noncompliant security groups. However, business units require SSH access and can provide a list of trusted IPs to restrict access.

Options:

## Options:

- A- Create a new AWS Systems Manager Automation runbook that adds an IP set to the security group's inbound rule. Update the AWS Config rule to change the automatic remediation action to use the new runbook.
- B- Create a new AWS Systems Manager Automation runbook that updates the security group's inbound rule with the IP addresses from the business units. Update the AWS Config rule to change the automatic remediation action to use the new runbook.
- C- Create an AWS Lambda function that adds an IP set to the security group's inbound rule. Update the AWS Config rule to change the automatic remediation action to use the Lambda function.
- D- Create an AWS Lambda function that updates the security group's inbound rule with the IP addresses from the business units. Update the AWS Config rule to change the automatic remediation action to use the Lambda function.

## Answer:

---

B

## Explanation:

---

The problem requires modifying the inbound SSH rule to restrict access to a list of trusted IPs instead of deleting it entirely. AWS Config rules can be configured with automatic remediation actions using either Systems Manager Automation runbooks or Lambda functions. However, AWS Systems Manager Automation runbooks are often more appropriate for managing infrastructure changes like security group modifications because they are reusable, parameterized, and easier to audit.

Create a Systems Manager Automation runbook: This runbook will contain steps to add or modify the existing security group rule, allowing SSH access only from the specified IP addresses.

Update the AWS Config rule: Modify the Config rule to call this new runbook for its automatic remediation. This will prevent deletion of the SSH rule and instead update it based on the IP list.

## Question 2

---

Question Type: MultipleChoice

---

[Deployment, Provisioning, and Automation]

A company is using an Amazon EC2 Auto Scaling group to support a workload. The company now needs to centrally manage access to the Auto Scaling group. The group is configured with two similar scaling policies (A and B) to centrally manage access. Policy A adds 5 instances when CPU utilization reaches 80%. The other policy (B) can connect to the external network when CPU utilization reaches 80%.

What will happen when CPU utilization reaches the 80% threshold?

### Options:

---

- A- Amazon EC2 Auto Scaling will add 5 instances
- B- Amazon EC2 Auto Scaling will add 10 instances
- C- Amazon EC2 Auto Scaling will add 15 instances.
- D- The Auto Scaling group will not scale because of conflicting policies

### Answer:

---

B

### Explanation:

---

Scaling Policies in Auto Scaling:

When multiple scaling policies trigger at the same time, each policy is executed independently.

If both policies are set to add 5 instances when CPU utilization reaches 80%, they will both be executed when the threshold is met.

Therefore, the total number of instances added will be the sum of the instances specified in both policies.

In this case, 5 instances from one policy and 5 instances from the other policy will result in a total of 10 instances being added.

Steps to Configure and Verify Scaling Policies:

Go to the AWS Management Console.

Navigate to EC2 and select 'Auto Scaling Groups.'

Select your Auto Scaling group and review the scaling policies.

Ensure that both scaling policies are configured to trigger at 80% CPU utilization.

Monitor the Auto Scaling group's activity to verify the addition of instances when the CPU utilization threshold is reached.

Scaling Policies for Amazon EC2 Auto Scaling

## Question 3

---

Question Type: MultipleChoice

---

[Security and Compliance]

A company that uses AWS Organizations recently implemented AWS Control Tower. The company now needs to centralize identity management. A SysOps administrator must federate AWS IAM Identity Center with an external SAML 2.0 identity provider (IdP) to centrally manage access to all the company's accounts and cloud applications.

Which prerequisites must the SysOps administrator have so that the SysOps administrator can connect to the external IdP? (Select TWO.)

### Options:

---

- A- A copy of the IAM Identity Center SAML metadata
- B- The IdP metadata, including the public X.509 certificate
- C- The IP address of the IdP
- D- Root access to the management account
- E- Administrative permissions to the member accounts of the organization

### Answer:

---

A, B

### Explanation:

---

IAM Identity Center SAML Metadata:

This metadata is required to establish the trust relationship between AWS IAM Identity Center and the external SAML 2.0 identity provider.

Steps:

Download the IAM Identity Center SAML metadata from the AWS Management Console.

Provide this metadata to the external IdP.

IdP Metadata:

The metadata from the IdP, including the public X.509 certificate, is needed to configure the trust relationship.

Steps:

Obtain the IdP metadata, which includes the entity ID, endpoints, and X.509 certificate.

Configure the IAM Identity Center with this information.

Configuring SAML 2.0 Federation with AWS IAM Identity Center

## Question 4

---

Question Type: MultipleChoice

---

[Monitoring, Reporting, and Automation]

A company is running a development application on an Amazon EC2 instance. The application uploads 500,000 files that are 1 GB in size into a large Amazon S3 bucket that has default encryption enabled. The EC2 instance is in the same AWS Region where the S3 bucket is deployed.

The company uses performance logging that is built into the application software. The logs show that the application is constantly waiting for the files to be written to the S3 bucket. A SysOps administrator needs to improve the application's throughput performance. The SysOps administrator validates that the networking on the EC2 instance is not constrained.

What should the SysOps administrator do to improve the S3 upload performance?"

Options:

---

- A- Enable S3 Transfer Acceleration on the S3 bucket.
- B- Split the S3 write operations to use multiple bucket prefixes to write items in parallel.
- C- Configure AWS PrivateLink for Amazon S3. Turn off encryption on the S3 bucket.
- D- Configure AWS Global Accelerator in the Region. Turn off encryption on the S3 bucket.

Answer:

---

B

Explanation:

---

Improve S3 Upload Performance:

Using multiple bucket prefixes can improve throughput by allowing parallel upload streams.

Steps:

Modify the application to write files to different prefixes in the S3 bucket.

Example: Instead of writing all files to `s3://bucket-name/`, write to `s3://bucket-name/prefix1/`, `s3://bucket-name/prefix2/`, etc.

Best Practices for Amazon S3 Performance

## Question 5

---

Question Type: MultipleChoice

---

[Monitoring, Reporting, and Automation]

A SysOps administrator needs to update an AWS account name. What should the SysOps administrator do to accomplish this goal?

### Options:

- A- Add the Administrator Access policy to the SysOps administrator's IAM user.
- B- Add the AWS\_ConfigRole policy to the SysOps administrator's IAM user.
- C- Change the AWS account name through the AWS Trusted Advisor interface.
- D- Sign in as the AWS account root user to make the change.

### Answer:

---

D

### Explanation:

---

Update AWS Account Name:

The AWS account name can only be changed by the root user of the account.

Steps:

Sign in to the AWS Management Console using the root user credentials.

Navigate to the 'My Account' page.

Update the account name field and save the changes.

Updating the AWS Account Name

## Question 6

---

Question Type: MultipleChoice

---

[Monitoring, Reporting, and Automation]

A company's architecture team must receive immediate email notification whenever new Amazon EC2 Instances are launched in the company's main AWS production account

What should a SysOps administrator do to meet this requirement?

### Options:

---

A- Create a user data script that sends an email message through a smart host connector. Include the architecture team's email address in the user data script as the recipient. Ensure that all new EC2 instances include the user data script as part of a standardized build process.

B- Create an Amazon Simple Notification Service (Amazon SNS) topic and a subscription that uses the email protocol. Enter the architecture team's email address as the subscriber. Create an Amazon EventBridge rule that reacts when EC2 instances are launched. Specify the SNS topic as the rule's target.

C- Create an Amazon Simple Queue Service (Amazon SQS) queue and a subscription that uses the email protocol. Enter the architecture team's email address as the subscriber. Create an Amazon EventBridge rule that reacts when EC2 instances are launched. Specify the SQS queue as the rule's target.

D- Create an Amazon Simple Notification Service (Amazon SNS) topic. Configure AWS Systems Manager to publish EC2 events to the SNS topic. Create an AWS Lambda function to poll the SNS topic. Configure the Lambda function to send any messages to the architecture team's email address.

### Answer:

---

B

### Explanation:

---

Create an SNS Topic and Subscription:

Amazon SNS allows you to send notifications to multiple endpoints.

Steps:

Go to the AWS Management Console.

Navigate to SNS and create a new topic.

Create a subscription for the topic using the email protocol.

Enter the architecture team's email address as the subscriber.

Amazon SNS

Create an EventBridge Rule:

Amazon EventBridge can monitor events and trigger actions.

Steps:

Go to the AWS Management Console.

Navigate to EventBridge.

Create a new rule that reacts to EC2 instance launch events.

Specify the SNS topic as the rule's target.

## Question 7

---

Question Type: MultipleChoice

---

[Deployment, Provisioning, and Automation]

A company uses AWS Cloud Formation to deploy its infrastructure. The company recently retired an application. A cloud operations engineer initiates CloudFormation stack deletion, and the stack gets stuck in DELETE FAILED status.

A SysOps administrator discovers that the stack had deployed a security group. The security group is referenced by other security groups in the environment. The SysOps administrator needs to delete the stack without affecting other applications.

Which solution will meet these requirements in the MOST operationally efficient manner?

### Options:

---

- A- Create a new security group that has a different name. Apply identical rules to the new security group. Replace all other security groups that reference the new security group. Delete the stack.
- B- Create a CloudFormation change set to delete the security group. Deploy the change set.
- C- Delete the stack again. Specify that the security group be retained.
- D- Perform CloudFormation drift detection. Delete the stack.

## Answer:

---

C

## Explanation:

---

Retain the Security Group:

When deleting a CloudFormation stack, you can specify resources to be retained instead of deleted.

Steps:

Go to the AWS Management Console.

Navigate to CloudFormation and select the stack.

Choose to delete the stack.

In the deletion options, specify that the security group should be retained.

This will delete the stack but keep the security group, ensuring no impact on other applications.

Deleting a Stack

## Question 8

---

Question Type: MultipleChoice

---

[Networking and Content Delivery]

A SysOps administrator is responsible for more than 50 Amazon EC2 instances that are deployed in a single production AWS account. The EC2 instances are running several different operating systems. The company's standards require patching to be completed at least once a month.

The SysOps administrator wants to use AWS Systems Manager to reduce the number of hours the company spends on operating system patching each month.

Which combination of steps should the SysOps administrator take to meet these requirements? (Select THREE.)

## Options:

---

A- Group similar EC2 instances together into resource groups by using AWS Resource Groups

B- Create a schedule in Systems Manager Patch Manager. Specify the appropriate resource group as

the target

C- Specify Systems Manager Automation runbooks to patch the operating systems. Register the runbooks as tasks in the maintenance window. Specify the appropriate resource group as the target

D- Create a Systems Manager Automation runbook to monitor and control the state of the patches required. Apply the runbook to Systems Manager Patch Manager

E- Create a single Systems Manager maintenance window for each resource group.

F- Configure Systems Manager Fleet Manager to apply a Systems Manager Automation runbook to the appropriate resource group.

### Answer:

---

A, B, E

### Explanation:

---

Group EC2 Instances Using Resource Groups:

Resource groups help organize and manage AWS resources based on tags and other criteria.

Steps:

Go to the AWS Management Console.

Navigate to AWS Resource Groups.

Create resource groups for similar EC2 instances based on tags or other criteria.

AWS Resource Groups

Create a Schedule in Patch Manager:

AWS Systems Manager Patch Manager automates the process of patching managed instances.

Steps:

Go to the AWS Management Console.

Navigate to Systems Manager and select Patch Manager.

Create a patch baseline if not already created.

Create a schedule for patching and specify the resource group as the target.

Create Maintenance Windows for Resource Groups:

Maintenance windows define a period of time for performing administrative tasks on instances.

Steps:

Go to the AWS Management Console.

Navigate to Systems Manager and select Maintenance Windows.

Create a maintenance window for each resource group.

Specify tasks and targets (resource groups) for each maintenance window.

## Question 9

---

Question Type: MultipleChoice

---

[Monitoring, Reporting, and Automation]

A company is using an Amazon CloudWatch alarm to monitor the FreeLocalStorage metric for an Amazon Aurora PostgreSQL production database. The alarm goes into ALARM state and indicates that the database is running low on temporary storage. A SysOps administrator discovers that a weekly report is using most of the temporary storage that is currently allocated.

What should the SysOps administrator do to solve this problem?

### Options:

---

- A- Turn on Aurora PostgreSQL query plan management.
- B- Modify the configuration of the DB cluster to turn on storage auto scaling.
- C- Add an Aurora read replica to the DB cluster. Modify the report to use the new read replica.
- D- Modify the DB instance class for each DB instance in the DB cluster to increase the instance size.

### Answer:

---

B

### Explanation:

---

Storage Auto Scaling:

Aurora storage auto scaling automatically increases the storage capacity of the database cluster when free storage space is running low.

Steps:

Go to the AWS Management Console.

Navigate to RDS and select your Aurora DB cluster.

Modify the DB cluster configuration to enable storage auto scaling.

Apply the changes.

Aurora Storage Auto Scaling



# Thank You for trying SOA-C02 PDF Demo

To try our SOA-C02 practice exam software visit  
link below

<https://prepbolt.com/SOA-C02.html>

## Start Your SOA-C02 Preparation

Use Coupon “**SAVE50**” for extra 50% discount on the purchase of Practice Test Software. Test your SOA-C02 preparation with actual exam questions.