

Valid Exam SOA-C02 Preparation | SOA-C02 Detail Explanation



BONUS!!! Download part of Actual4Exams SOA-C02 dumps for free: https://drive.google.com/open?id=1SOsaS_i3R3cyIyv_FQTDMoLR7GaHy_Q0

Actual4Exams has a strong IT elite team. They use their professional eyes searching the latest SOA-C02 braindumps and SOA-C02 certification training materials. With them, you can save more time to study and pass the SOA-C02 Exam. After you purchase our SOA-C02 exam dumps, we will offer free update service in one year.

Amazon SOA-C02 (AWS Certified SysOps Administrator - Associate) exam is designed for individuals who want to validate their skills and knowledge in managing and operating systems on the AWS platform. SOA-C02 exam is intended for candidates who have at least one year of hands-on experience in managing and operating AWS systems, as well as a strong understanding of AWS services and infrastructure.

Amazon SOA-C02, also known as the AWS Certified SysOps Administrator - Associate certification exam, is a highly sought-after credential for professionals seeking to validate their knowledge and skills in managing and operating systems on the Amazon Web Services (AWS) platform. AWS Certified SysOps Administrator - Associate (SOA-C02) certification exam is designed for individuals who have a strong understanding of AWS core services and can manage and operate systems on the platform efficiently.

>> Valid Exam SOA-C02 Preparation <<

Amazon SOA-C02 Detail Explanation & Discount SOA-C02 Code

Our SOA-C02 learning guide materials have always been synonymous with excellence. Our SOA-C02 practice guide can help users achieve their goals easily, regardless of whether you want to pass various qualifying examination, our products can provide you with the learning materials you want. Of course, our SOA-C02 Real Questions can give users not only valuable experience about the exam, but also the latest information about the exam. Our SOA-C02 practical material is a learning tool that produces a higher yield than the other. If you make up your mind, choose us!

The AWS Certified SysOps Administrator - Associate (SOA-C02) certification exam is designed for IT professionals who want to demonstrate their expertise in deploying, managing, and operating applications on the AWS platform. SOA-C02 exam covers a wide range of topics, including monitoring, deployment, automation, security, networking, and troubleshooting. Passing SOA-C02 Exam demonstrates that the candidate has the skills and knowledge required to effectively manage and operate applications on AWS.

Amazon AWS Certified SysOps Administrator - Associate (SOA-C02) Sample Questions (Q563-Q568):

NEW QUESTION # 563

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. Enable Amazon GuardDuty. Configure S3 protection to monitor all data inside Amazon S3.
- B. Create an AWS Config rule to discover sensitive personal information in the S3 files and mark them as noncompliant.
- **C. Enable Amazon Macie. Create a discovery job that uses the managed data identifier.**
- D. Create an S3 event-driven artificial intelligence/machine learning (AI/ML) pipeline to classify sensitive personal information by using Amazon Recognition.

Answer: C

Explanation:

Amazon Macie is a security service designed to help organizations find, classify, and protect sensitive data stored in Amazon S3. Amazon Macie uses machine learning to automatically discover, classify, and protect sensitive data in Amazon S3. Creating a discovery job with the managed data identifier will allow Macie to identify sensitive personal information in the S3 files and classify it accordingly. Enabling AWS Config and Amazon GuardDuty will not help with this requirement as they are not designed to automatically classify and protect data.

NEW QUESTION # 564

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 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.**
- 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 inbound endpoint.
Create a conditional forwarding rule on the on-premises DNS servers to forward DNS requests for example.com to the inbound endpoints.

Answer: A

Explanation:

We want to forward DNS queries to an on-prem DNS server, we need to create a Route53 outbound resolver endpoint. The last step of the configuration process is to associate the rule with a VPC (not necessarily the same where we created the outbound endpoint).

<https://aws.amazon.com/premiumsupport/knowledge-center/route53-resolve-with-outbound-endpoint/>

NEW QUESTION # 565

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

Answer: C

NEW QUESTION # 566

Lab Simulation 5

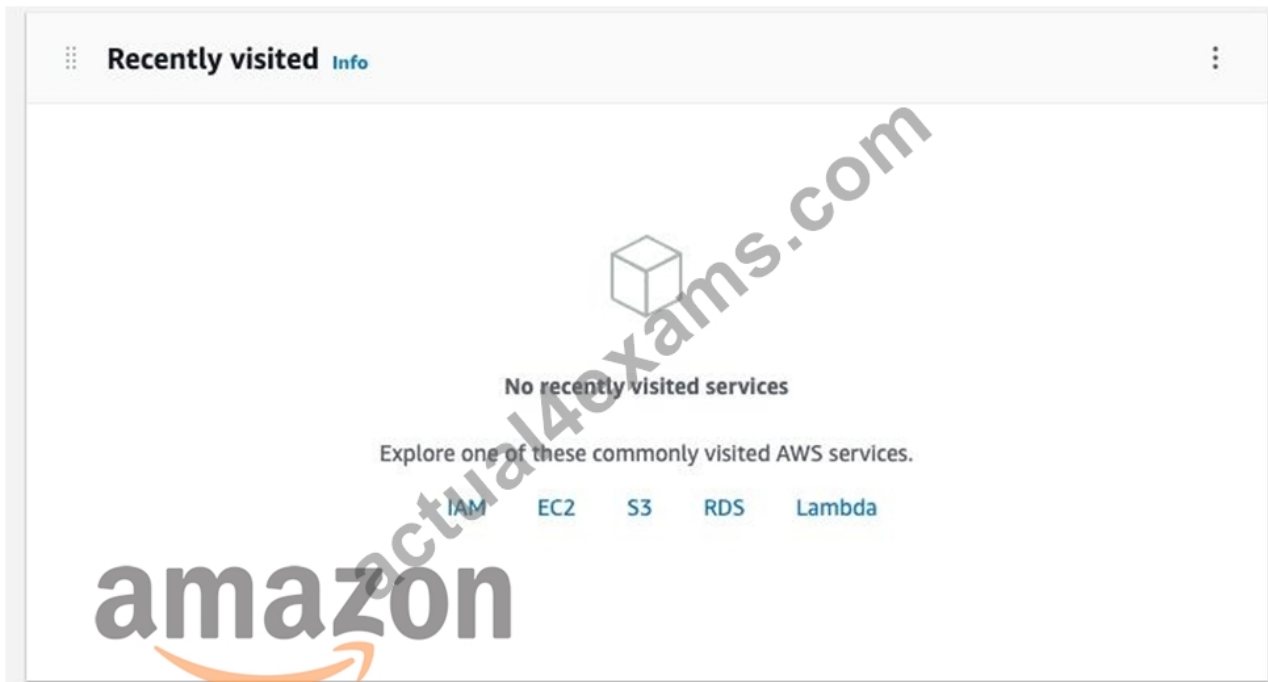
Instructions.

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.

Create a solution to automate Amazon EBS Volume snapshots using Amazon Data Lifecycle Manager.

1. Use the us-east-2 Region for all resources.
 2. Unless specified below, use the default configuration settings.
 3. Create a snapshot of the existing EBS Volume named OriginalVolume.
 4. Create a 1 GB EBS Volume from the snapshot with default encryption.
 5. Add the tag Snapshot:true to the new EBS Volume.
 6. Ensure that snapshots of all volumes with the tag Snapshot:true are taken every 6 hours and retained for 90 days. Do NOT use a cron expression. Ensure this is the only lifecycle policy that exists. Use the IAM role named DLMRole.
- Important: Click the Next button to complete this lab and continue to the next lab. Once you click the Next button, you will NOT be able to return to this lab.



New EC2 Experience ×
Tell us what you think

EC2 Dashboard

- EC2 Global View
- Events
- Tags
- Limits
- ▶ **Instances**
 - Instances
- ▼ **Images**
 - AMIs
 - AMI Catalog
- ▼ **Elastic Block Store**
 - Volumes
 - Snapshots
 - Lifecycle Manager
- ▼ **Network & Security**
 - Security Groups
 - Elastic IPs
 - Placement Groups

Resources EC2 Global view ↻ ⚙️

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	0	Auto Scaling Groups	0	Dedicated Hosts	0
Elastic IPs	0	Instances	0	Key pairs	0
Load balancers	0	Placement groups	0	Security groups	0
Snapshots	0	Volumes	1		

ⓘ Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. [Learn more](#) ×

Launch instance
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance ▼

[Migrate a server](#) ↗

Service health

↻ [AWS Health Dashboard](#) ↗

Region
US East (Ohio)

Status
✔ This service is operating normally

New EC2 Experience ×
Tell us what you think

EC2 Dashboard

- EC2 Global View
- Events
- Tags
- Limits
- ▶ **Instances**
 - Instances
- ▼ **Images**
 - AMIs
 - AMI Catalog
- ▼ **Elastic Block Store**
 - Volumes
 - Snapshots
 - Lifecycle Manager
- ▼ **Network & Security**
 - Security Groups
 - Elastic IPs
 - Placement Groups

ⓘ You can now create Amazon Data Lifecycle Manager policies to automate snapshot management directly from this screen. Select the volumes to back up, and then choose **Actions**, **Create snapshot lifecycle policy**. For more information, see the [Knowledge Center article](#). ×

Volumes (1) ↻ **Actions** ▲ **Create volume**

🔍 Filter volumes

<input type="checkbox"/>	Name ▼	Volume ID ▼	Type ▼	Size ▼	IOPS ▼	Throughput ▼
<input type="checkbox"/>	OriginalVolume	vol-0f9a5f6a3a6bd464c	gp3	1 GiB	3000	125

Create snapshot [Info](#)

Create a point-in-time snapshot to back up the data on an Amazon EBS volume to Amazon S3.



Volume ID

 vol-0f9a5f6a3a6bd464e (OriginalVolume)

Description

Add a description for your snapshot

255 characters maximum.

Encryption [Info](#)

Not encrypted

Tags [Info](#)

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

[Add tag](#)

You can add 50 more tags.

Cancel

Create snapshot

Volume settings

Snapshot ID

 snap-037fa9927babb858f

Volume type [Info](#)

General Purpose SSD (gp2) ▼

Size (GiB) [Info](#)

1

Min: 1 GiB, Max: 16384 GiB. The value must be an integer.

IOPS [Info](#)

100 / 3000

Based on 100 GiB per GiB with a maximum of 100 IOPS, burstable to 3000 IOPS.

Throughput (MiB/s) [Info](#)

Not applicable

Availability Zone [Info](#)

us-east-2a 

Fast snapshot restore [Info](#)

Not enabled for selected snapshot

Encryption [Info](#)

Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances.

Encrypt this volume

KMS key

(default)aws/ebs ▲ 

Tags - optional [Info](#)

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Snapshot X

Value - optional

true X

Remove

Add tag

You can add 50 more tags.

Cancel

Create volume

Volume settings

Snapshot ID

[snap-037fa9927babb858f](#)

Volume type [Info](#)

General Purpose SSD (gp2) ▼

Size (GiB) [Info](#)

1

Min: 1 GiB, Max: 16384 GiB. The value must be an integer.

IOPS [Info](#)

100 / 3000

Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS.

Throughput (MiB/s) [Info](#)

Not applicable

Availability Zone [Info](#)

us-east-2a ▼



Fast snapshot restore [Info](#)

Not enabled for selected snapshot

Encryption [Info](#)

Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances.

Encrypt this volume

KMS key

(default)aws/ebs ▲



KMS key description

Default key that protects my EBS volumes when no other key is defined

KMS key owner

292309197860 (This account)

KMS key ID

a0c7e5ee-8189-4542-b553-b2b883e6d2e6

KMS key ARN

arn:aws:kms:us-east-2:292309197860:key/a0c7e5ee-8189-4542-b553-b2b883e6d2e6

Volumes that are created from encrypted snapshots are automatically encrypted using the same key as the snapshot, or using a different key that you specify. Volumes that are created from unencrypted snapshots are automatically unencrypted, but you can choose to encrypt them using a specific key. If no snapshot is selected, you can choose to encrypt the volume and specify your own key. [Learn More](#)

amazon

Compute

Amazon Data Lifecycle Manager

Automate the creation, retention, copy and deletion of snapshots and AMIs

Amazon Data Lifecycle Manager provides a simple, automated way to back up data stored on Amazon EBS volumes.



Create new lifecycle policy

Policy type

EBS snapshot policy

Next step

Benefits and features

Automated snapshot and AMI creation

Create a policy that automates the creation, retention, and deletion of EBS snapshots and EBS-backed AMIs.

Fast snapshot restore integration

Automate the creation of snapshots that are enabled for fast snapshot restore. Fast snapshot restore enables you to restore volumes that are fully initialized at creation and instantly deliver all of their provisioned performance.

Step 1

Specify settings

Step 2

Configure schedule 1 -
Schedule 1

Step 3

Review and create

Specify settings

Target resources Info

Specify the resources that are to be targeted by this policy.

Target resource types

Select the type of resources that are to be targeted.

- Volume
- Instance

Target resource tags

All resources of the selected type that have at least one of these tags will be targeted by the policy.

Snapshot
true

45 tags remaining of 45.

Description

Policy description

IAM role Info

This policy must be associated with an IAM role that has the appropriate permissions. If you choose to create a new role, you must grant relevant role permissions and set up trust relationships correctly. If you are unsure of what role to use, choose Default role.

Default role

i If the default role already exists, Amazon Data Lifecycle Manager will use that role. If it does not exist yet, it will be automatically created with all the required permissions.

▶ View default role permissions

Choose another role

Tags - optional Info

Assign custom tags to the policy to help you identify, organize, and secure your lifecycle policies. Each tag consists of a key and an optional value.

No tags associated with the resource.

You can add up to 50 more tags.

Policy status

Specify whether to enable the policy immediately after creation or modification. If you do not enable the policy now, then it will not begin creating snapshots or AMIs until you manually set its activation status to enabled.

- Enabled
- Not enabled

Step 2
Configure schedule 1 - Schedule 1

Step 3
 Review and create

You can add 3 more schedules to this policy. They must have the same retention type as Schedule 1, but they can have their own retention count or age. Snapshot archiving can be enabled for one schedule only.

Schedule details [Info](#) Remove schedule Add another schedule

Schedule name

Frequency

Every

Starting at
 UTC

Retention type
 snapshots in standard tier

Step 2
Configure schedule 1 - Schedule 1

Step 3
 Review and create

You can add 3 more schedules to this policy. They must have the same retention type as Schedule 1, but they can have their own retention count or age. Snapshot archiving can be enabled for one schedule only.

Schedule details [Info](#) Remove schedule Add another schedule

Schedule name

Frequency

Every

Starting at
 UTC

Retention type
 days after creation

Advanced settings – optional

- ▶ Tagging [Info](#)
- ▶ Snapshot archiving [Info](#)
- ▶ Fast snapshot restore [Info](#)
- ▶ Cross-Region copy [Info](#)
- ▶ Cross-account sharing [Info](#)

Step 2
Configure schedule 1 -
Schedule 1

You can add 3 more schedules to this policy. They must have the same retention type as Schedule 1, but they can have their own retention count or age. Snapshot archiving can be enabled for one schedule only.

Step 3
Review and create

Step 1: Policy settings

Modify

Policy details

Target resource types	Target resource tags
Volume	Snapshot:true
Description	Role name
description	DLMRole
Policy status	Policy tags
Enabled	-

Step 2: Schedule 1 configuration

Modify

Schedule details

Schedule name

Schedule 1

Frequency

Every 12 hour(s) starting at 09:00

Retention in standard tier

90 days after creation

Cancel

Previous

Create policy

	Name	Policy ID	Description	Policy type	State
<input type="checkbox"/>	-	policy-043a371896095b320	description	EBS snapshot policy	Enabled

Answer:

Explanation:

P.S. Free & New SOA-C02 dumps are available on Google Drive shared by Actual4Exams: https://drive.google.com/open?id=1SOsaS_i3R3cyIyv_FQTDMoLR7GaHy_Q0