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.pass2lead.com/soa-c02.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A company updates its security policy to prohibit the public exposure of any data in Amazon S3 buckets in the company\\'s account. What should a SysOps administrator do to meet this requirement?

A. Turn on S3 Block Public Access from the account level.

B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to enforce that all S3 objects are private.

C. Use Amazon Inspector to search for S3 buckets and to automatically reset S3 ACLs if any public S3 buckets are found.

D. Use S3 Object Lambda to examine S3 ACLs and to change any public S3 ACLs to private.

Correct Answer: A

S3 Block Public Access is a security feature that can be enabled at the account level to prevent public access to S3 buckets and objects. It provides four settings for blocking public access, which can be applied at the account level, the bucket

level, or the object level. By enabling this feature at the account level, all existing and future S3 buckets and objects will be protected against public access. This meets the requirement to prohibit the public exposure of any data in S3 buckets

in the company\\'s account.

https://aws.amazon.com/s3/features/block-public-access/

QUESTION 2

A company has a large on-premises tape backup solution. The company has started to use AWS Storage Gateway. The company created a Tape Gateway to replace the existing on-premises hardware. The company\\'s backup engineer noticed that some of the backup jobs that were supposed to write to AWS failed to run because of a "Not Enough Space" error.

The company does not want these failures to happen again. The company also wants to consistently have enough tape available on AWS.

What is the MOST operationally efficient way for a SysOps administrator to meet these requirements?

A. Create an AWS Lambda function that runs on an hourly basis and checks how many tapes have available space. If the available tapes are below a certain threshold, provision more.

B. Install the Amazon CloudWatch agent on the on-premises system. Push the log files to a CloudWatch log group. Create an AWS Lambda function that creates more tapes when the "Not Enough Space" error appears. Create a metric filter and a metric alarm that launches the Lambda function.

C. Create an additional Tape Gateway with its own set of tapes. Configure Amazon Simple Notification Service (Amazon SNS) to send a notification to the backup engineer if the tapes that are associated with the primary Tape Gateway do not have available space.

D. Configure tape auto-create on the Tape Gateway. In the auto-create settings, configure a minimum number of tapes, an appropriate barcode prefix, and a tape pool.

Correct Answer: D

The Tape Gateway automatically creates new virtual tapes to maintain the minimum number of available tapes that you configure. It then makes these new tapes available for import by the backup application so that your backup jobs can run without interruption. Automatic tape creation removes the need for custom scripting in addition to the manual process for creating new virtual tapes. https://docs.aws.amazon.com/storagegateway/latest/tgw/managing-automatic-tape-creation.html

QUESTION 3

A large company is using AWS Organizations to manage hundreds of AWS accounts across multiple AWS Regions. The company has turned on AWS Config throughout the organization.

The company requires all Amazon S3 buckets to block public read access. A SysOps administrator must generate a monthly report that shows all the S3 buckets and whether they comply with this requirement.

Which combination of steps should the SysOps administrator take to collect this data? {Select TWO).

A. Create an AWS Config aggregator in an aggregator account. Use the organization as the source. Retrieve the compliance data from the aggregator.

B. Create an AWS Config aggregator in each account. Use an S3 bucket in an aggregator account as the destination. Retrieve the compliance data from the S3 bucket

C. Edit the AWS Config policy in AWS Organizations. Use the organization\\'s management account to turn on the s3-bucket-public-read-prohibited rule for the entire organization.

D. Use the AWS Config compliance report from the organization\\'s management account. Filter the results by resource, and select Amazon S3.

E. Use the AWS Config API to apply the s3-bucket-public-read-prohibited rule in all accounts for all available Regions.

Correct Answer: CD

QUESTION 4

A company is using an Amazon DynamoDB table for data. A SysOps administrator must configure replication of the table to another AWS Region for disaster recovery. What should the SysOps administrator do to meet this requirement?

A. Enable DynamoDB Accelerator (DAX).

B. Enable DynamoDB Streams, and add a global secondary index (GSI).

C. Enable DynamoDB Streams, and-add a global table Region.

D. Enable point-in-time recovery.

Correct Answer: C

QUESTION 5

A company is using Amazon Elastic File System (Amazon EFS) to share a file system among several Amazon EC2 instances. As usage increases, users report that file retrieval from the EFS file system is slower than normal. Which action should a SysOps administrator take to improve the performance of the file system?

A. Configure the file system for Provisioned Throughput.

B. Enable encryption in transit on the file system.

C. Identify any unused files in the file system, and remove the unused files.

D. Resize the Amazon Elastic Block Store (Amazon EBS) volume of each of the EC2 instances.

Correct Answer: A

QUESTION 6

An organization with a large IT department has decided to migrate to AWS With different job functions in the IT department it is not desirable to give all users access to all AWS resources Currently the organization handles access via LDAP group membership

What is the BEST method to allow access using current LDAP credentials?

A. Create an AWS Directory Service Simple AD Replicate the on-premises LDAP directory to Simple AD

B. Create a Lambda function to read LDAP groups and automate the creation of IAM users

C. Use AWS CloudFormation to create IAM roles Deploy Direct Connect to allow access to the on-premises LDAP server

D. Federate the LDAP directory with IAM using SAML Create different IAM roles to correspond to different LDAP groups to limit permissions

Correct Answer: D

QUESTION 7

A company hosts a database on an Amazon RDS Multi-AZ DB instance. The database is not encrypted. The company\\'s new security policy requires all AWS resources to be encrypted at rest and in transit.

What should a SysOps administrator do to encrypt the database?

A. Configure encryption on the existing DB instance.

B. Take a snapshot of the DB instance. Encrypt the snapshot. Restore the snapshot to the same DB instance.

C. Encrypt the standby replica in a secondary Availability Zone. Promote the standby replica to the primary DB instance.

D. Take a snapshot of the DB instance. Copy and encrypt the snapshot. Create a new DB instance by restoring the encrypted copy.

Correct Answer: B

QUESTION 8

A company has a web application that is experiencing performance problems many times each night. A root cause analysis reveals sudden increases in CPU utilization that last 5 minutes on an Amazon EC2 Linux instance. A SysOps

administrator must find the process ID (PID) of the service or process that is consuming more CPU.

What should the SysOps administrator do to collect the process utilization information with the LEAST amount of effort?

A. Configure the Amazon CloudWatch agent procstat plugin to capture CPU process metrics.

B. Configure an AWS Lambda function to run every minute to capture the PID and send a notification.

C. Log in to the EC2 instance by using a .pem key each night. Then run the top command.

D. Use the default Amazon CloudWatch CPU utilization metric to capture the PID in CloudWatch.

Correct Answer: A

The procstat plugin enables you to collect metrics from individual processes. It is supported on Linux servers and on servers running Windows Server 2012 or later.
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Agent-procstat-process-metrics.html

QUESTION 9

A company has a compliance requirement that no security groups can allow SSH ports to be open to all IP addresses. A SysOps administrator must implement a solution that will notify the company\\'s SysOps team when a security group rule violates this requirement. The solution also must remediate the security group rule automatically.

Which solution will meet these requirements?

A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function when a security group changes. Configure the Lambda function to evaluate the security group for compliance, remove all inbound security group rules on all ports, and notify the SysOps team if the security group is noncompliant.

B. Create an AWS CloudTrail metric filter for security group changes. Create an Amazon CloudWatch alarm to notify the SysOps team through an Amazon Simple Notification Service (Amazon SNS) topic when (he metric is greater than 0. Subscribe an AWS Lambda function to the SNS topic to remediate the security group rule by removing the rule.

C. Activate the AWS Config restricted-ssh managed rule. Add automatic remediation to the AWS Config rule by using the AWS Systems Manager Automation AWS- DisablePublicAccessForSecurityGroup runbook. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to notify the SysOps team when the rule is noncompliant.

D. Create an AWS CloudTrail metric filter for security group changes. Create an Amazon CloudWatch alarm for when the metric is greater than 0. Add an AWS Systems Manager action to the CloudWatch alarm to suspend the security group by using the Systems Manager Automation AWS-DisablePublicAccessForSecurityGroup runbook when the alarm is in ALARM state. Add an Amazon Simple Notification Service (Amazon SNS) topic as a second target to notify the SysOps team.

Correct Answer: C

Checks if the incoming SSH traffic for the security groups is accessible. The rule is COMPLIANT when IP addresses of the incoming SSH traffic in the security groups are restricted (CIDR other than 0.0.0.0/0). This rule applies only to IPv4.

Identifier: INCOMING_SSH_DISABLED

Resource Types: AWS::EC2::SecurityGroup

Trigger type: Configuration changes

QUESTION 10

A SysOps administrator wants to upload a file that is 1 TB in size from on-premises to an Amazon S3 bucket using multipart uploads. What should the SysOps administrator do to meet this requirement?

A. Upload the file using the S3 console.

B. Use the s3api copy-object command.

C. Use the s3api put-object command.

D. Use the s3 cp command.

Correct Answer: D

It\\'s a best practice to use aws s3 commands (such as aws s3 cp) for multipart uploads and downloads, because these aws s3 commands automatically perform multipart uploading and downloading based on the file size. By comparison, aws s3api commands, such as aws s3api create-multipart-upload, should be used only when aws s3 commands don\\'t support a specific upload need, such as when the multipart upload involves multiple servers, a multipart upload is manually stopped and resumed later, or when the aws s3 command doesn\\'t support a required request parameter. https://aws.amazon.com/premiumsupport/knowledge-center/s3-multipart-upload-cli/

QUESTION 11

A SysOps administrator needs to control access to groups of Amazon EC2 instances using AWS Systems Manager Session Manager. Specific tags on the EC2 instances have already been added. Which additional actions should the administrator take to control access? (Choose two.)

A. Attach an IAM policy to the users or groups that require access to the EC2 instances.

B. Attach an IAM role to control access to the EC2 instances.

C. Create a placement group for the EC2 instances and add a specific tag.

D. Create a service account and attach it to the EC2 instances that need to be controlled.

E. Create an IAM policy that grants access to any EC2 instances with a tag specified in the Condition element.

Correct Answer: BE

In the navigation pane, choose Roles, and then choose Create role.

In the navigation pane, choose Roles, and then choose the existing role you want to associate with an instance profile for Systems Manager operations.

On the Permissions tab, choose Add permissions, Attach policies.

https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-instance-profile.html

The instance role for the instances must reference a policy that allows access to the appropriate services; you can create your own or use AmazonSSMManagedInstanceCore.

https://aws.amazon.com/blogs/aws/new-session-manager/

Attach the IAM role to your private EC2 instance.

https://aws.amazon.com/premiumsupport/knowledge-center/ec2-systems-manager-vpc-endpoints/

QUESTION 12

A SysOps administrator is using AWS CloudFormation StackSets to create AWS resources in two AWS Regions in the same AWS account. A stack operation fails in one Region and returns the stack instance status of OUTDATED. What is the cause of this failure?

A. The CloudFormation template changed on the local disk and has not been submitted to CloudFormation.

B. The CloudFormation template is trying to create a global resource that is not unique.

C. The stack has not yet been deployed to the Region.

D. The SysOps administrator is using an old version of the CloudFormation API.

Correct Answer: B

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stacksets-troubleshooting.html

QUESTION 13

A company wants to collect data from an application to use for analytics. For the first 90 days, the data will be infrequently accessed but must remain highly available. During this time, the company\\'s analytics team requires access to the data in milliseconds. However, after 90 days, the company must retain the data for the long term at a lower cost. The retrieval time after 90 days must be less than 5 hours.

Which solution will meet these requirements MOST cost-effectively?

A. Store the data in S3 Standard-Infrequent Access (S3 Standard-IA) for the first 90 days. Set up an S3 Lifecycle rule to move the data to S3 Glacier Flexible Retrieval after 90 days.

B. Store the data in S3 One Zone-Infrequent Access (S3 One Zone-IA) for the first 90 days. Set up an S3 Lifecycle rule to move the data to S3 Glacier Deep Archive after 90 days.

C. Store the data in S3 Standard for the first 90 days. Set up an S3 Lifecycle rule to move the data to S3 Glacier Flexible Retrieval after 90 days.

D. Store the data in S3 Standard for the first 90 days. Set up an S3 Lifecycle rule to move the data to S3 Glacier Deep Archive after 90 days.

Correct Answer: A

S3 Glacier Flexible Retrieval provides three retrieval options: expedited retrievals that typically complete in 1–5 minutes,

standard retrievals that typically complete in 3–5 hours, and free bulk retrievals that return large amounts of data typically in 5–12 hours.

The Amazon S3 Glacier Deep Archive storage class provides two retrieval options ranging from 12-48 hours.

QUESTION 14

A company is using an Amazon Aurora MySQL DB cluster that has point-in-time recovery, backtracking, and automatic backup enabled. A SysOps administrator needs to be able to roll back the DB cluster to a specific recovery point within the previous 72 hours. Restores must be completed in the same production DB cluster.

Which solution will meet these requirements?

A. Create an Aurora Replica. Promote the replica to replace the primary DB instance.

B. Create an AWS Lambda function to restore an automatic backup to the existing DB cluster.

C. Use backtracking to rewind the existing DB cluster to the desired recovery point.

D. Use point-in-time recovery to restore the existing DB cluster to the desired recovery point.

Correct Answer: C

"The limit for a backtrack window is 72 hours.....Backtracking is only available for DB clusters that were created with the Backtrack feature enabled....Backtracking "rewinds" the DB cluster to the time you specify. Backtracking is not a replacement for backing up your DB cluster so that you can restore it to a point in time....You can backtrack a DB cluster quickly. Restoring a DB cluster to a point in time launches a new DB cluster and restores it from backup data or a DB cluster snapshot, which can take hours."

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Managi ng.Backtrack.html

QUESTION 15

A SysOps administrator needs to deploy an application in multiple AWS Regions. The SysOps administrator must implement a solution that routes users to the Region with the lowest latency. In case of failure, the solution must automatically route requests to a Region with a healthy instance of the application. The company needs a solution with the shortest time to failover.

Which solution will meet these requirements?

A. Create Amazon Route 53 A records that have the same name for each endpoint. Use a latency routing policy. Associate a health check with each record.

B. Create Amazon Route 53 A records that have the same name for each endpoint. Use a failover routing policy. Associate a health check with each record.

C. Create an AWS Global Accelerator standard accelerator. Create an endpoint group for each Region. Add a listener to the accelerator. Associate the endpoint group with the listener.

D. Create Amazon Route 53 A records that have the same name for each endpoint. Use a geolocation routing policy. Associate a health check with each record.

Correct Answer: C

AWS Global Accelerator is a service that helps to improve the availability and performance of applications by directing traffic through the AWS global network. It automatically routes traffic to the closest AWS Region based on the lowest

latency for the end user.

By creating an endpoint group for each AWS Region, the Global Accelerator can distribute traffic across multiple Regions. This means that users will be routed to the Region with the lowest latency, ensuring the best performance for their

location.

Adding a listener to the accelerator allows it to listen for incoming traffic and direct it to the appropriate endpoint group.

The AWS Global Accelerator constantly monitors the health of the endpoints (applications) in each endpoint group. If an endpoint becomes unhealthy or experiences a failure, the Global Accelerator automatically reroutes traffic to a healthy

instance of the application in another Region, ensuring high availability and automatic failover.

Latest SOA-C02 Dumps SOA-C02 PDF Dumps SOA-C02 VCE Dumps