

Amazon Web Services

Exam Questions SOA-C02

AWS Certified SysOps Administrator - Associate (SOA-C02)



NEW QUESTION 1

- (Exam Topic 1)

A SysOps administrator receives an alert from Amazon GuardDuty about suspicious network activity on an Amazon EC2 instance. The GuardDuty finding lists a new external IP address as a traffic destination. The SysOps administrator does not recognize the external IP address. The SysOps administrator must block traffic to the external IP address that GuardDuty identified.

Which solution will meet this requirement?

- A. Create a new security group to block traffic to the external IP address
- B. Assign the new security group to the EC2 instance.
- C. Use VPC flow logs with Amazon Athena to block traffic to the external IP address.
- D. Create a network ACL
- E. Add an outbound deny rule for traffic to the external IP address.
- F. Create a new security group to block traffic to the external IP address
- G. Assign the new security group to the entire VPC.

Answer: C

Explanation:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html>

NEW QUESTION 2

- (Exam Topic 1)

A SysOps administrator applies the following policy to an AWS CloudFormation stack:

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "Update:*",
      "Principal": "*",
      "Resource": ["LogicalResourceId/Production*"]
    },
    {
      "Effect": "Allow",
      "Action": "Update:*",
      "Principal": "*",
      "Resource": "*"
    }
  ]
}
```

What is the result of this policy?

- A. Users that assume an IAM role with a logical ID that begins with "Production" are prevented from running the update-stack command.
- B. Users can update all resources in the stack except for resources that have a logical ID that begins with "Production".
- C. Users can update all resources in the stack except for resources that have an attribute that begins with "Production".
- D. Users in an IAM group with a logical ID that begins with "Production" are prevented from running the update-stack command.

Answer: B

NEW QUESTION 3

- (Exam Topic 1)

A company needs to archive all audit logs for 10 years. The company must protect the logs from any future edits.

Which solution will meet these requirements?

- A. Store the data in an Amazon Elastic Block Store (Amazon EBS) volume
- B. Configure AWS Key Management Service (AWS KMS) encryption.
- C. Store the data in an Amazon S3 Glacier vault
- D. Configure a vault lock policy for write-once, read-many (WORM) access.
- E. Store the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA). Configure server-side encryption.
- F. Store the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA). Configure multi-factor authentication (MFA).

Answer: B

Explanation:

To meet the requirements of the workload, a company should store the data in an Amazon S3 Glacier vault and configure a vault lock policy for write-once, read-many (WORM) access. This will ensure that the data is stored securely and cannot be edited in the future. The other solutions (storing the data in an Amazon Elastic Block Store (Amazon EBS) volume and configuring AWS Key Management Service (AWS KMS) encryption, storing the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA) and configuring server-side encryption, or storing the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA) and configuring multi-factor authentication (MFA)) will not meet the requirements, as they do not provide a way to protect the audit logs from future edits.

https://docs.aws.amazon.com/zh_tw/AmazonS3/latest/userguide/object-lock.html

NEW QUESTION 4

- (Exam Topic 1)

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

Answer: D

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 5

- (Exam Topic 1)

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

NEW QUESTION 6

- (Exam Topic 1)

A database is running on an Amazon RDS Multi-AZ DB instance. A recent security audit found the database to be out of compliance because it was not encrypted. Which approach will resolve the encryption requirement?

- A. Log in to the RDS console and select the encryption box to encrypt the database
- B. Create a new encrypted Amazon EBS volume and attach it to the instance
- C. Encrypt the standby replica in the secondary Availability Zone and promote it to the primary instance.
- D. Take a snapshot of the RDS instance, copy and encrypt the snapshot and then restore to the new RDS instance

Answer: D

NEW QUESTION 7

- (Exam Topic 1)

A SysOps administrator wants to manage a web server application with AWS Elastic Beanstalk. The Elastic Beanstalk service must maintain full capacity for new deployments at all times.

Which deployment policies satisfy this requirement? (Select TWO.)

- A. All at once
- B. Immutable
- C. Rebuild
- D. Rolling
- E. Rolling with additional batch

Answer: BE

Explanation:

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.rolling-version-deploy.html>

NEW QUESTION 8

- (Exam Topic 1)

A company uses AWS Organizations to manage its AWS accounts. A SysOps administrator must create a backup strategy for all Amazon EC2 instances across all the company's AWS accounts.

Which solution will meet these requirements In the MOST operationally efficient way?

- A. Deploy an AWS Lambda function to each account to run EC2 instance snapshots on a scheduled basis.
- B. Create an AWS CloudFormation stack set in the management account to add an AutoBackup=True tag to every EC2 instance
- C. Use AWS Backup In the management account to deploy policies for all accounts and resources.
- D. Use a service control policy (SCP) to run EC2 instance snapshots on a scheduled basis in each account.

Answer: B

NEW QUESTION 9

- (Exam Topic 1)

A company uses an Amazon S3 bucket to store data files. The S3 bucket contains hundreds of objects. The company needs to replace a tag on all the objects in the S3 bucket with another tag.

What is the MOST operationally efficient way to meet this requirement?

- A. Use S3 Batch Operation
- B. Specify the operation to replace all object tags.
- C. Use the AWS CLI to get the tags for each object
- D. Save the tags in a list
- E. Use S3 Batch Operations. Specify the operation to delete all object tags
- F. Use the AWS CLI and the list to retag the objects.
- G. Use the AWS CLI to get the tags for each object
- H. Save the tags in a list
- I. Use the AWS CLI and the list to remove the object tags
- J. Use the AWS CLI and the list to retag the objects.
- K. Use the AWS CLI to copy the objects to another S3 bucket
- L. Add the new tag to the copied objects. Delete the original objects.

Answer: A

Explanation:

Ref. <https://aws.amazon.com/es/blogs/storage/adding-and-removing-object-tags-with-s3-batch-operations/>

NEW QUESTION 10

- (Exam Topic 1)

While setting up an AWS managed VPN connection, a SysOps administrator creates a customer gateway resource in AWS. The customer gateway device resides in a data center with a NAT gateway in front of it.

What address should be used to create the customer gateway resource?

- A. The private IP address of the customer gateway device
- B. The MAC address of the NAT device in front of the customer gateway device
- C. The public IP address of the customer gateway device
- D. The public IP address of the NAT device in front of the customer gateway device

Answer: D

NEW QUESTION 11

- (Exam Topic 1)

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 over utilized 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

NEW QUESTION 12

- (Exam Topic 1)

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.

Answer: A

NEW QUESTION 13

- (Exam Topic 1)

A company manages an application that uses Amazon ElastiCache for Redis with two extra-large nodes spread across two different Availability Zones. The company's IT team discovers that the ElastiCache for Redis cluster has 75% freeable memory. The application must maintain high availability.

What is the MOST cost-effective way to resize the cluster?

- A. Decrease the number of nodes in the ElastiCache for Redis cluster from 2 to 1.
- B. Deploy a new ElastiCache for Redis cluster that uses large node type
- C. Migrate the data from the original cluster to the new cluster
- D. After the process is complete, shut down the original cluster.
- E. Deploy a new ElastiCache for Redis cluster that uses large node type
- F. Take a backup from the original cluster, and restore the backup in the new cluster
- G. After the process is complete, shut down the original cluster.
- H. Perform an online resizing for the ElastiCache for Redis cluster
- I. Change the node types from extra-large nodes to large nodes.

Answer: D

Explanation:

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/scaling-redis-cluster-mode-enabled.html> As demand on your clusters changes, you might decide to improve performance or reduce costs by changing the number of shards in your Redis (cluster mode enabled) cluster. We recommend using online horizontal scaling to do so, because it allows your cluster to continue serving requests during the scaling process.
<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/redis-cluster-vertical-scaling-scaling-down.html>

NEW QUESTION 14

- (Exam Topic 1)

An application runs on multiple Amazon EC2 instances in an Auto Scaling group. The Auto Scaling group is configured to use the latest version of a launch template. A SysOps administrator must devise a solution that centrally manages the application logs and retains the logs for no more than 90 days. Which solution will meet these requirements?

- A. Launch an Amazon Machine Image (AMI) that is preconfigured with the Amazon CloudWatch Logs agent to send logs to an Amazon S3 bucket. Apply a 90-day S3 Lifecycle policy on the S3 bucket to expire the application logs.
- B. Launch an Amazon Machine Image (AMI) that is preconfigured with the Amazon CloudWatch Logs agent to send logs to a log group. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled rule to perform an instance refresh every 90 days.
- C. Update the launch template user data to install and configure the Amazon CloudWatch Logs agent to send logs to a log group. Configure the retention period on the log group to be 90 days.
- D. Update the launch template user data to install and configure the Amazon CloudWatch Logs agent to send logs to a log group. Set the log rotation configuration of the EC2 instances to 90 days.

Answer: C

NEW QUESTION 15

- (Exam Topic 1)

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 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

NEW QUESTION 16

- (Exam Topic 1)

A company has a public website that recently experienced problems. Some links led to missing webpages, and other links rendered incorrect webpages. The application infrastructure was running properly, and all the provisioned resources were healthy. Application logs and dashboards did not show any errors, and no monitoring alarms were raised. Systems administrators were not aware of any problems until end users reported the issues.

The company needs to proactively monitor the website for such issues in the future and must implement a solution as soon as possible.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Rewrite the application to surface a custom error to the application log when issues occur. Automatically parse logs for error.
- B. Create an Amazon CloudWatch alarm to provide alerts when issues are detected.
- C. Create an AWS Lambda function to test the website.
- D. Configure the Lambda function to emit an Amazon CloudWatch custom metric when errors are detected.
- E. Configure a CloudWatch alarm to provide alerts when issues are detected.
- F. Create an Amazon CloudWatch Synthetic canary.
- G. Use the CloudWatch Synthetic Recorder plugin to generate the script for the canary run.
- H. Configure the canary in line with requirements.
- I. Create an alarm to provide alerts when issues are detected.

Answer: A

NEW QUESTION 17

- (Exam Topic 1)

A SysOps administrator is designing a solution for an Amazon RDS for PostgreSQL DB instance. Database credentials must be stored and rotated monthly. The applications that connect to the DB instance send

write-intensive traffic with variable client connections that sometimes increase significantly in a short period of time.

Which solution should a SysOps administrator choose to meet these requirements?

- A. Configure AWS Key Management Service (AWS KMS) to automatically rotate the keys for the DB instance.
- B. Use RDS Proxy to handle the increases in database connections.
- C. Configure AWS Key Management Service (AWS KMS) to automatically rotate the keys for the DB instance.
- D. Use RDS read replicas to handle the increases in database connections.
- E. Configure AWS Secrets Manager to automatically rotate the credentials for the DB instance.
- F. Use RDS Proxy to handle the increases in database connections.
- G. Configure AWS Secrets Manager to automatically rotate the credentials for the DB instance.
- H. Use RDS read replicas to handle the increases in database connections.

Answer: A

NEW QUESTION 18

- (Exam Topic 1)

A company recently purchased Savings Plans. The company wants to receive email notification when the company's utilization drops below 90% for a given day. Which solution will meet this requirement?

- A. Create an Amazon CloudWatch alarm to monitor the Savings Plan check in AWS Trusted Advisor. Configure an Amazon Simple Queue Service (Amazon SQS) queue for email notification when the utilization drops below 90% for a given day.
- B. Create an Amazon CloudWatch alarm to monitor the SavingsPlansUtilization metric under the AWS/SavingsPlans namespace in CloudWatc
- C. Configure an Amazon Simple Queue Service (Amazon SQS) queue for email notification when the utilization drops below 90% for a given day.
- D. Create a Savings Plans alert to monitor the daily utilization of the Savings Plan
- E. Configure an Amazon Simple Notification Service (Amazon SNS) topic for email notification when the utilization drops below 90% for a given day.
- F. Use AWS Budgets to create a Savings Plans budget to track the daily utilization of the Savings Plans. Configure an Amazon Simple Notification Service (Amazon SNS) topic for email notification when the utilization drops below 90% for a given day.

Answer: D

Explanation:

AWS Budgets can be used to create a Savings Plans budget and track the daily utilization of the company's Savings Plans. By creating a budget, it will trigger an action when the utilization drops below 90%, which in this case will be to send an email notification via an Amazon SNS topic. This will ensure that the company is notified when their Savings Plans utilization drops below 90%, allowing them to take action if necessary.

Reference: [1] <https://docs.aws.amazon.com/savingsplans/latest/userguide/sp-usingBudgets.html>

NEW QUESTION 19

- (Exam Topic 1)

A company uses Amazon Elasticsearch Service (Amazon ES) to analyze sales and customer usage data. Members of the company's geographically dispersed sales team are traveling. They need to log in to Kibana by using their existing corporate credentials that are stored in Active Directory. The company has deployed Active Directory Federation Services (AD FS) to enable authentication to cloud services. Which solution will meet these requirements?

- A. Configure Active Directory as an authentication provider in Amazon E
- B. Add the Active Directory server's domain name to Amazon E
- C. Configure Kibana to use Amazon ES authentication.
- D. Deploy an Amazon Cognito user poo
- E. Configure Active Directory as an external identity provider for the user poo
- F. Enable Amazon Cognito authentication for Kibana on Amazon ES.
- G. Enable Active Directory user authentication in Kiban
- H. Create an IP-based custom domain access policy in Amazon ES that includes the Active Directory server's IP address.
- I. Establish a trust relationship with Kibana on the Active Directory serve
- J. Enable Active Directory user authentication in Kiban
- K. Add the Active Directory server's IP address to Kibana.

Answer: B

Explanation:

<https://aws.amazon.com/blogs/security/how-to-enable-secure-access-to-kibana-using-aws-single-sign-on/> <https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-cognito-auth.html>

NEW QUESTION 20

- (Exam Topic 1)

A company has an application that runs only on Amazon EC2 Spot Instances. The instances run in an Amazon EC2 Auto Scaling group with scheduled scaling actions.

However, the capacity does not always increase at the scheduled times, and instances terminate many times a day. A Sysops administrator must ensure that the instances launch on time and have fewer interruptions.

Which action will meet these requirements?

- A. Specify the capacity-optimized allocation strategy for Spot Instance
- B. Add more instance types to the Auto Scaling group.
- C. Specify the capacity-optimized allocation strategy for Spot Instance
- D. Increase the size of the instances in the Auto Scaling group.
- E. Specify the lowest-price allocation strategy for Spot Instance
- F. Add more instance types to the Auto Scaling group.
- G. Specify the lowest-price allocation strategy for Spot Instance
- H. Increase the size of the instances in the Auto Scaling group.

Answer: A

Explanation:

Specifying the capacity-optimized allocation strategy for Spot Instances and adding more instance types to the Auto Scaling group is the best action to meet the requirements. Increasing the size of the instances in the Auto Scaling group will not necessarily help with the launch time or reduce interruptions, as the Spot Instances could still be interrupted even with larger instance sizes.

NEW QUESTION 21

- (Exam Topic 1)

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 (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

NEW QUESTION 22

- (Exam Topic 1)

A company monitors its account activity using AWS CloudTrail. and is concerned that some log files are being tampered with after the logs have been delivered to the account's Amazon S3 bucket.

Moving forward, how can the SysOps administrator confirm that the log files have not been modified after being delivered to the S3 bucket?

- A. Stream the CloudTrail logs to Amazon CloudWatch Logs to store logs at a secondary location.
- B. Enable log file integrity validation and use digest files to verify the hash value of the log file.
- C. Replicate the S3 log bucket across regions, and encrypt log files with S3 managed keys.
- D. Enable S3 server access logging to track requests made to the log bucket for security audits.

Answer: B

Explanation:

When you enable log file integrity validation, CloudTrail creates a hash for every log file that it delivers. Every hour, CloudTrail also creates and delivers a file that references the log files for the last hour and contains a hash of each. This file is called a digest file. CloudTrail signs each digest file using the private key of a public and private key pair. After delivery, you can use the public key to validate the digest file. CloudTrail uses different key pairs for each AWS region

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html>

NEW QUESTION 23

- (Exam Topic 1)

A company is running a serverless application on AWS Lambda The application stores data in an Amazon RDS for MySQL DB instance Usage has steadily increased and recently there have been numerous "too many connections" errors when the Lambda function attempts to connect to the database The company already has configured the database to use the maximum max_connections value that is possible

What should a SysOps administrator do to resolve these errors'?

- A. Create a read replica of the database Use Amazon Route 53 to create a weighted DNS record that contains both databases
- B. Use Amazon RDS Proxy to create a proxy Update the connection string in the Lambda function
- C. Increase the value in the max_connect_errors parameter in the parameter group that the database uses
- D. Update the Lambda function's reserved concurrency to a higher value

Answer: B

Explanation:

<https://aws.amazon.com/blogs/compute/using-amazon-rds-proxy-with-aws-lambda/>

RDS Proxy acts as an intermediary between your application and an RDS database. RDS Proxy establishes and manages the necessary connection pools to your database so that your application creates fewer database connections. Your Lambda functions interact with RDS Proxy instead of your database instance. It handles the connection pooling necessary for scaling many simultaneous connections created by concurrent Lambda functions. This allows your Lambda applications to reuse existing connections, rather than creating new connections for every function invocation.

Check "Database proxy for Amazon RDS" section in the link to see how RDS proxy help Lambda handle huge connections to RDS MySQL

<https://aws.amazon.com/blogs/compute/using-amazon-rds-proxy-with-aws-lambda/>

NEW QUESTION 24

- (Exam Topic 1)

A company needs to view a list of security groups that are open to the internet on port 3389. What should a SysOps administrator do to meet this requirement?

- A. Configure Amazon GuardDuty to scan security groups and report unrestricted access on port 3389.
- B. Configure a service control policy (SCP) to identify security groups that allow unrestricted access on port 3389.
- C. Use AWS Identity and Access Management Access Analyzer to find any instances that have unrestricted access on port 3389.
- D. Use AWS Trusted Advisor to find security groups that allow unrestricted access on port 3389

Answer: D

NEW QUESTION 25

- (Exam Topic 1)

A company hosts a web portal on Amazon EC2 instances. The web portal uses an Elastic Load Balancer (ELB) and Amazon Route 53 for its public DNS service. The ELB and the EC2 instances are deployed by way of a single AWS CloudFormation stack in the us-east-1 Region. The web portal must be highly available across multiple Regions.

Which configuration will meet these requirements?

- A. Deploy a copy of the stack in the us-west-2 Regio
- B. Create a single start of authority (SOA) record in Route 53 that includes the IP address from each EL
- C. Configure the SOA record with health check
- D. Use the ELB in us-east-1 as the primary record and the ELB in us-west-2 as the secondary record.
- E. Deploy a copy of the stack in the us-west-2 Regio
- F. Create an additional A record in Route 53 that includes the ELB in us-west-2 as an alias targe
- G. Configure the A records with a failover routing policy and health check
- H. Use the ELB in us-east-1 as the primary record and the ELB in us-west-2 as the secondary record.
- I. Deploy a new group of EC2 instances in the us-west-2 Regio
- J. Associate the new EC2 instances with the existing ELB, and configure load balancer health checks on all EC2 instance
- K. Configure the ELB to update Route 53 when EC2 instances in us-west-2 fail health checks.
- L. Deploy a new group of EC2 instances in the us-west-2 Regio
- M. Configure EC2 health checks on all EC2 instances in each Regio
- N. Configure a peering connection between the VPC
- O. Use the VPC in us-east-1 as the primary record and the VPC in us-west-2 as the secondary record.

Answer: B

Explanation:

When you create a hosted zone, Route 53 automatically creates a name server (NS) record and a start of authority (SOA) record for the zone.
<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/migrate-dns-domain-in-use.html#migrate-dns-crea>
https://en.wikipedia.org/wiki/SOA_record

NEW QUESTION 26

- (Exam Topic 1)

A company recently migrated its application to a VPC on AWS. An AWS Site-to-Site VPN connection connects the company's on-premises network to the VPC. The application retrieves customer data from another system that resides on premises. The application uses an on-premises DNS server to resolve domain records. After the migration, the application is not able to connect to the customer data because of name resolution errors. Which solution will give the application the ability to resolve the internal domain names?

- A. Launch EC2 instances in the VP
- B. On the EC2 instances, deploy a custom DNS forwarder that forwards all DNS requests to the on-premises DNS serve
- C. Create an Amazon Route 53 private hosted zone that uses the EC2 instances for name servers.
- D. Create an Amazon Route 53 Resolver outbound endpoint
- E. Configure the outbound endpoint to forward DNS queries against the on-premises domain to the on-premises DNS server.
- F. Set up two AWS Direct Connect connections between the AWS environment and the on-premises network
- G. Set up a link aggregation group (LAG) that includes the two connection
- H. Change the VPC resolver address to point to the on-premises DNS server.
- I. Create an Amazon Route 53 public hosted zone for the on-premises domain
- J. Configure the network ACLs to forward DNS requests against the on-premises domain to the Route 53 public hosted zone.

Answer: B

Explanation:

https://docs.aws.amazon.com/zh_tw/Route53/latest/DeveloperGuide/resolver-forwarding-outbound-queries.html

NEW QUESTION 27

- (Exam Topic 1)

A company has a VPC with public and private subnets. An Amazon EC2 based application resides in the private subnets and needs to process raw .csv files stored in an Amazon S3 bucket. A SysOps administrator has set up the correct IAM role with the required permissions for the application to access the S3 bucket, but the application is unable to communicate with the S3 bucket. Which action will solve this problem while adhering to least privilege access?

- A. Add a bucket policy to the S3 bucket permitting access from the IAM role.
- B. Attach an S3 gateway endpoint to the VPC
- C. Configure the route table for the private subnet.
- D. Configure the route table to allow the instances on the private subnet access through the internet gateway.
- E. Create a NAT gateway in a private subnet and configure the route table for the private subnets.

Answer: B

Explanation:

Technology to use is a VPC endpoint - "A VPC endpoint enables private connections between your VPC and supported AWS services and VPC endpoint services powered by AWS PrivateLink. AWS PrivateLink is a technology that enables you to privately access services by using private IP addresses. Traffic between your VPC and the other service does not leave the Amazon network." S3 is an example of a gateway endpoint. We want to see services in AWS while not leaving the VPC.

NEW QUESTION 28

- (Exam Topic 1)

A SysOps administrator uses AWS Systems Manager Session Manager to connect to instances. After the SysOps administrator launches a new Amazon EC2 instance, the EC2 instance does not appear in the Session Manager list of systems that are available for connection. The SysOps administrator verifies that Systems Manager Agent is installed, updated, and running on the EC2 instance. What is the reason for this issue?

- A. The SysOps administrator does not have access to the key pair that is required for connection.
- B. The SysOps administrator has not attached a security group to the EC2 instance to allow SSH on port 22.
- C. The EC2 instance does not have an attached IAM role that allows Session Manager to connect to the EC2 instance.
- D. The EC2 instance ID has not been entered into the Session Manager configuration.

Answer: C

NEW QUESTION 29

- (Exam Topic 1)

A company hosts an online shopping portal in the AWS Cloud. The portal provides HTTPS security by using a TLS certificate on an Elastic Load Balancer (ELB). Recently, the portal suffered an outage because the TLS certificate expired. A SysOps administrator must create a solution to automatically renew certificates to avoid this issue in the future. What is the MOST operationally efficient solution that meets these requirements?

- A. Request a public certificate by using AWS Certificate Manager (ACM). Associate the certificate from ACM with the ELB.
- B. Write a scheduled AWS Lambda function to renew the certificate every 18 months.
- C. Request a public certificate by using AWS Certificate Manager (ACM). Associate the certificate from ACM with the ELB.
- D. ACM will automatically manage the renewal of the certificate.
- E. Register a certificate with a third-party certificate authority (CA). Import this certificate into AWS Certificate Manager (ACM). Associate the certificate from ACM with the ELB.
- F. ACM will automatically manage the renewal of the certificate.

- G. Register a certificate with a third-party certificate authority (CA). Configure the ELB to import the certificate directly from the C
- H. Set the certificate refresh cycle on the ELB to refresh when the certificate is within 3 months of the expiration date.

Answer: B

Explanation:

"A certificate is eligible for automatic renewal subject to the following considerations: ELIGIBLE if associated with another AWS service, such as Elastic Load Balancing or CloudFront. ELIGIBLE if exported since being issued or last renewed. ELIGIBLE if it is a private certificate issued by calling the ACM RequestCertificate API and then exported or associated with another AWS service. ELIGIBLE if it is a private certificate issued through the management console and then exported or associated with another AWS service." <https://docs.aws.amazon.com/acm/latest/userguide/managed-renewal.html>

NEW QUESTION 30

- (Exam Topic 1)

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

NEW QUESTION 31

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SOA-C02 Practice Exam Features:

- * SOA-C02 Questions and Answers Updated Frequently
- * SOA-C02 Practice Questions Verified by Expert Senior Certified Staff
- * SOA-C02 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * SOA-C02 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SOA-C02 Practice Test Here](#)