

# Amazon

## Exam Questions AWS-SysOps

Amazon AWS Certified SysOps Administrator - Associate



**NEW QUESTION 1**

- (Exam Topic 2)

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-2 Region 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 15 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 Path:

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

Input template:

"The EC2 Spot Instance <instance> has been on account."

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Here are the steps to configure Amazon EventBridge to meet the above requirements:

- Log in to the AWS Management Console by using the AWS Management Console shortcut from the VM desktop. Make sure that you are logged in to the desired AWS account.
- Go to the EventBridge service in the us-east-2 Region.
- In the EventBridge service, navigate to the "Event buses" page.
- Click on the "Create event bus" button.
- Give a name to your event bus, and select "default" as the event source type.
- Navigate to "Rules" page and create a new rule named "RunFunction"
- In the "Event pattern" section, select "Schedule" as the event source and set the schedule to run every 15 minutes.
- In the "Actions" section, select "Send to Lambda" and choose the existing AWS Lambda function named "LogEventFunction"
- Create another rule named "SpotWarning"
- In the "Event pattern" section, select "EC2" as the event source, and filter the events on "EC2 Spot Instance interruption"
- In the "Actions" section, select "Send to SNS topic" and create a new standard Amazon SNS topic named "TopicEvents"
- In the "Input Transformer" section, set the Input Path to {"instance" : "\$.detail.instance-id"} and Input template to "The EC2 Spot Instance <instance> has been interrupted on account."
- Now all Amazon EC2 events in the default event bus will be replayable for past 90 days. Note:
- You can use the AWS Management Console, AWS CLI, or SDKs to create and manage EventBridge resources.
- You can use CloudTrail event history to replay events from the past 90 days.
- You can refer to the AWS EventBridge documentation for more information on how to configure and use the service: <https://aws.amazon.com/eventbridge/>

**NEW QUESTION 2**

- (Exam Topic 1)

A SysOps administrator is using Amazon EC2 instances to host an application. The SysOps administrator needs to grant permissions for the application to access an Amazon DynamoDB table.

Which solution will meet this requirement?

- A. Create access keys to access the DynamoDB tabl
- B. Assign the access keys to the EC2 instance profile.
- C. Create an EC2 key pair to access the DynamoDB tabl
- D. Assign the key pair to the EC2 instance profile.
- E. Create an IAM user to access the DynamoDB tabl
- F. Assign the IAM user to the EC2 instance profile.
- G. Create an IAM role to access the DynamoDB tabl
- H. Assign the IAM role to the EC2 instance profile.

**Answer:** D

**NEW QUESTION 3**

- (Exam Topic 1)

A SysOps administrator has created an AWS Service Catalog portfolio and has shared the portfolio with a second AWS account in the company. The second account is controlled by a different administrator.

Which action will the administrator of the second account be able to perform?

- A. Add a product from the imported portfolio to a local portfolio.
- B. Add new products to the imported portfolio.
- C. Change the launch role for the products contained in the imported portfolio.
- D. Customize the products in the imported portfolio.

**Answer:** A

#### NEW QUESTION 4

- (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 5

- (Exam Topic 1)

A company has an internal web application that runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group in a single Availability Zone. A SysOps administrator must make the application highly available. Which action should the SysOps administrator take to meet this requirement?

- A. Increase the maximum number of instances in the Auto Scaling group to meet the capacity that is required at peak usage.
- B. Increase the minimum number of instances in the Auto Scaling group to meet the capacity that is required at peak usage.
- C. Update the Auto Scaling group to launch new instances in a second Availability Zone in the same AWS Region.
- D. Update the Auto Scaling group to launch new instances in an Availability Zone in a second AWS Region.

**Answer:** C

#### Explanation:

"An Auto Scaling group can contain EC2 instances in one or more Availability Zones within the same Region. However, Auto Scaling groups cannot span multiple Regions". As stated in <https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-benefits.htm>

#### NEW QUESTION 6

- (Exam Topic 1)

A SysOps administrator is notified that an Amazon EC2 instance has stopped responding. The AWS Management Console indicates that the system status checks are failing. What should the administrator do first to resolve this issue?

- A. Reboot the EC2 instance so it can be launched on a new host
- B. Stop and then start the EC2 instance so that it can be launched on a new host
- C. Terminate the EC2 instance and relaunch it
- D. View the AWS CloudTrail log to investigate what changed on the EC2 instance

**Answer:** B

#### Explanation:

<https://aws.amazon.com/premiumsupport/knowledge-center/ec2-windows-system-status-check-fail/>

#### NEW QUESTION 7

- (Exam Topic 1)

A company stores files on 50 Amazon S3 buckets in the same AWS Region. The company wants to connect to the S3 buckets securely over a private connection from its Amazon EC2 instances. The company needs a solution that produces no additional cost. Which solution will meet these requirements?

- A. Create a gateway VPC endpoint for each S3 bucket
- B. Attach the gateway VPC endpoints to each subnet inside the VPC.
- C. Create an interface VPC endpoint for each S3 bucket
- D. Attach the interface VPC endpoints to each subnet inside the VPC.
- E. Create one gateway VPC endpoint for all the S3 buckets
- F. Add the gateway VPC endpoint to the VPC route table.
- G. Create one interface VPC endpoint for all the S3 buckets
- H. Add the interface VPC endpoint to the VPC route table.

**Answer:** C

#### NEW QUESTION 8

- (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 VPC
- B. On the EC2 instances, deploy a custom DNS forwarder that forwards all DNS requests to the on-premises DNS server
- 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](https://docs.aws.amazon.com/zh_tw/Route53/latest/DeveloperGuide/resolver-forwarding-outbound-queries.html)

#### NEW QUESTION 9

- (Exam Topic 1)

A company runs an application on an Amazon EC2 instance. A SysOps administrator creates an Auto Scaling group and an Application Load Balancer (ALB) to handle an increase in demand. However, the EC2 instances are failing the health check. What should the SysOps administrator do to troubleshoot this issue?

- A. Verify that the Auto Scaling group is configured to use all AWS Regions.
- B. Verify that the application is running on the protocol and the port that the listener is expecting.
- C. Verify the listener priority in the ALB. Change the priority if necessary.
- D. Verify the maximum number of instances in the Auto Scaling group. Change the number if necessary.

**Answer: B**

#### NEW QUESTION 10

- (Exam Topic 1)

A company is expanding its fleet of Amazon EC2 instances before an expected increase of traffic. When a SysOps administrator attempts to add more instances, an InstanceLimitExceeded error is returned.

What should the SysOps administrator do to resolve this error?

- A. Add an additional CIDR block to the VPC.
- B. Launch the EC2 instances in a different Availability Zone.
- C. Launch new EC2 instances in another VPC.
- D. Use Service Quotas to request an EC2 quota increase.

**Answer: D**

#### NEW QUESTION 10

- (Exam Topic 1)

A SysOps administrator is optimizing the cost of a workload. The workload is running in multiple AWS Regions and is using AWS Lambda with Amazon EC2 On-Demand Instances for the compute. The overall usage is predictable. The amount of compute that is consumed in each Region varies, depending on the users' locations.

Which approach should the SysOps administrator use to optimize this workload?

- A. Purchase Compute Savings Plans based on the usage during the past 30 days
- B. Purchase Convertible Reserved Instances by calculating the usage baseline.
- C. Purchase EC2 Instance Savings Plan based on the usage during the past 30 days
- D. Purchase Standard Reserved Instances by calculating the usage baseline.

**Answer: C**

#### NEW QUESTION 13

- (Exam Topic 1)

A software development company has multiple developers who work on the same product. Each developer must have their own development environment, and these development environments must be identical. Each development environment consists of Amazon EC2 instances and an Amazon RDS DB instance. The development environments should be created only when necessary, and they must be terminated each night to minimize costs.

What is the MOST operationally efficient solution that meets these requirements?

- A. Provide developers with access to the same AWS CloudFormation template so that they can provision their development environment when necessary.
- B. Schedule a nightly cron job on each development instance to stop all running processes to reduce CPU utilization to nearly zero.
- C. Provide developers with access to the same AWS CloudFormation template so that they can provision their development environment when necessary.
- D. Schedule a nightly Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function to delete the AWS CloudFormation stacks.
- E. Provide developers with CLI commands so that they can provision their own development environment when necessary.
- F. Schedule a nightly Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function to terminate all EC2 instances and the DB instance.
- G. Provide developers with CLI commands so that they can provision their own development environment when necessary.
- H. Schedule a nightly Amazon EventBridge (Amazon CloudWatch Events) rule to cause AWS CloudFormation to delete all of the development environment resources.

**Answer: B**

#### NEW QUESTION 15

- (Exam Topic 1)

A company has a new requirement stating that all resources in AWS must be tagged according to a set policy. Which AWS service should be used to enforce and continually identify all resources that are not in compliance with the policy?

- A. AWS CloudTrail



- B. Amazon Inspector
- C. AWSConfig
- D. AWS Systems Manager

**Answer:** C

#### NEW QUESTION 16

- (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 helps Lambda handle huge connections to RDS MySQL.

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

#### NEW QUESTION 18

- (Exam Topic 1)

An Amazon EC2 instance is running an application that uses Amazon Simple Queue Service (Amazon SQS) queues. A SysOps administrator must ensure that the application can read, write, and delete messages from the SQS queues. Which solution will meet these requirements in the MOST secure manner?

- A. Create an IAM user with an IAM policy that allows the `sqs:SendMessage` permission, the `sqs:ReceiveMessage` permission, and the `sqs:DeleteMessage` permission to the appropriate queues. Embed the IAM user's credentials in the application's configuration.
- B. Create an IAM user with an IAM policy that allows the `sqs:SendMessage` permission, the `sqs:ReceiveMessage` permission, and the `sqs:DeleteMessage` permission to the appropriate queues. Export the IAM user's access key and secret access key as environment variables on the EC2 instance.
- C. Create and associate an IAM role that allows EC2 instances to call AWS services. Attach an IAM policy to the role that allows `sqs:` permissions to the appropriate queues.
- D. Create and associate an IAM role that allows EC2 instances to call AWS services. Attach an IAM policy to the role that allows the `sqs:SendMessage` permission, the `sqs:ReceiveMessage` permission, and the `sqs:DeleteMessage` permission to the appropriate queues.

**Answer:** D

#### NEW QUESTION 20

- (Exam Topic 1)

A SysOps administrator is deploying a test site running on Amazon EC2 instances. The application requires both incoming and outgoing connectivity to the internet.

Which combination of steps are required to provide internet connectivity to the EC2 instances? (Choose two.)

- A. Add a NAT gateway to a public subnet.
- B. Attach a private address to the elastic network interface on the EC2 instance.
- C. Attach an Elastic IP address to the internet gateway.
- D. Add an entry to the route table for the subnet that points to an internet gateway.
- E. Create an internet gateway and attach it to a VPC.

**Answer:** DE

#### Explanation:

[https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_Internet\\_Gateway.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html)

#### NEW QUESTION 25

- (Exam Topic 1)

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 inbound endpoint. Create a conditional forwarding rule on the on-premises DNS servers to forward DNS requests for example.com to the inbound endpoints.
- 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 server.
- C. Associate this rule with the VPC.
- D. 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.
- E. Create an Amazon Route 53 Resolver outbound endpoint.
- F. 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.

**Answer:** C

#### NEW QUESTION 27

- (Exam Topic 1)

A company wants to be alerted through email when IAM CreateUser API calls are made within its AWS account.

Which combination of actions should a SysOps administrator take to meet this requirement? (Choose two.)

- A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with AWS CloudTrail as the event source and IAM CreateUser as the specific API call for the event pattern.
- B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with Amazon CloudSearch as the event source and IAM CreateUser as the specific API call for the event pattern.
- C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with AWS IAM Access Analyzer as the event source and IAM CreateUser as the specific API call for the event pattern.
- D. Use an Amazon Simple Notification Service (Amazon SNS) topic as an event target with an email subscription.
- E. Use an Amazon Simple Email Service (Amazon SES) notification as an event target with an email subscription.

**Answer:** AD

#### Explanation:

<https://aws.amazon.com/blogs/security/how-to-receive-alerts-when-your-iam-configuration-changes/>

#### NEW QUESTION 31

- (Exam Topic 1)

A company is managing multiple AWS accounts in AWS Organizations. The company is reviewing internal security of its AWS environment. The company's security administrator has their own AWS account and wants to review the VPC configuration of developer AWS accounts.

Which solution will meet these requirements in the MOST secure manner?

- A. Create an IAM policy in each developer account that has read-only access related to VPC resources. Assign the policy to an IAM user. Share the user credentials with the security administrator.
- B. Create an IAM policy in each developer account that has administrator access to all Amazon EC2 actions, including VPC actions. Assign the policy to an IAM user. Share the user credentials with the security administrator.
- C. Create an IAM policy in each developer account that has administrator access related to VPC resources. Assign the policy to a cross-account IAM role. Ask the security administrator to assume the role from their account.
- D. Create an IAM policy in each developer account that has read-only access related to VPC resources. Assign the policy to a cross-account IAM role. Ask the security administrator to assume the role from their account.

**Answer:** D

#### NEW QUESTION 33

- (Exam Topic 1)

A company runs an application on Amazon EC2 instances. The EC2 instances are in an Auto Scaling group and run behind an Application Load Balancer (ALB). The application experiences errors when total requests exceed 100 requests per second. A SysOps administrator must collect information about total requests for a 2-week period to determine when requests exceeded this threshold.

What should the SysOps administrator do to collect this data?

- A. Use the ALB's RequestCount metric.
- B. Configure a time range of 2 weeks and a period of 1 minute. Examine the chart to determine peak traffic times and volumes.
- C. Use Amazon CloudWatch metric math to generate a sum of request counts for all the EC2 instances over a 2-week period.
- D. Sort by a 1-minute interval.
- E. Create Amazon CloudWatch custom metrics on the EC2 launch configuration templates to create aggregated request metrics across all the EC2 instances.
- F. Create an Amazon EventBridge (Amazon CloudWatch Events) rule.
- G. Configure an EC2 event matching pattern that creates a metric that is based on EC2 request.
- H. Display the data in a graph.

**Answer:** A

#### Explanation:

Using the ALB's RequestCount metric will allow the SysOps administrator to collect information about total requests for a 2-week period and determine when requests exceeded the threshold of 100 requests per second. Configuring a time range of 2 weeks and a period of 1 minute will ensure that the data can be accurately examined to determine peak traffic times and volumes.

#### NEW QUESTION 37

- (Exam Topic 1)

A SysOps administrator is required to monitor free space on Amazon EBS volumes attached to Microsoft Windows-based Amazon EC2 instances within a company's account. The administrator must be alerted to potential issues.

What should the administrator do to receive email alerts before low storage space affects EC2 instance performance?

- A. Use built-in Amazon CloudWatch metrics, and configure CloudWatch alarms and an Amazon SNS topic for email notifications.
- B. Use AWS CloudTrail logs and configure the trail to send notifications to an Amazon SNS topic.
- C. Use the Amazon CloudWatch agent to send disk space metrics, then set up CloudWatch alarms using an Amazon SNS topic.
- D. Use AWS Trusted Advisor and enable email notification alerts for EC2 disk space.

**Answer:** C

#### NEW QUESTION 39

- (Exam Topic 1)

A company needs to create a daily Amazon Machine Image (AMI) of an existing Amazon Linux EC2 instance that hosts the operating system, application, and database on multiple attached Amazon Elastic Block Store (Amazon EBS) volumes. File system integrity must be maintained.

Which solution will meet these requirements?

- A. Create an AWS Lambda function to call the CreateImage API operation with the EC2 instance ID and the no-reboot parameter enable
- B. Create a daily scheduled Amazon EventBridge (Amazon CloudWatch Events) rule that invokes the function.
- C. Create an AWS Lambda function to call the CreateImage API operation with the EC2 instance ID and the reboot parameter enable
- D. Create a daily scheduled Amazon EventBridge (Amazon CloudWatch Events) rule that invokes the function.
- E. Use AWS Backup to create a backup plan with a backup rule that runs dail
- F. Assign the resource ID of the EC2 instance with the no-reboot parameter enabled.
- G. Use AWS Backup to create a backup plan with a backup rule that runs dail
- H. Assign the resource ID of the EC2 instance with the reboot parameter enabled.

**Answer: B**

**Explanation:**

[https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/Creating\\_EBSbacked\\_WinAMI.html](https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/Creating_EBSbacked_WinAMI.html) "NoReboot By default, Amazon EC2 attempts to shut down and reboot the instance before creating the image.

If the No Reboot option is set, Amazon EC2 doesn't shut down the instance before creating the image. When this option is used, file system integrity on the created image can't be guaranteed." Besides, we can use AWS EventBridge to invoke Lambda function

[https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API\\_CreateImage.html](https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_CreateImage.html)

**NEW QUESTION 42**

- (Exam Topic 1)

A SysOps administrator configures an Amazon S3 gateway endpoint in a VPC. The private subnets inside the VPC do not have outbound internet access. A user logs in to an Amazon EC2 instance in one of the private subnets and cannot upload a file to an Amazon S3 bucket in the same AWS Region

Which solution will solve this problem?

- A. Update the EC2 instance role policy to allow s3:PutObject access to the target S3 bucket.
- B. Update the EC2 security group to allow outbound traffic to 0.0.0.0/0 for port 80.
- C. Update the EC2 subnet route table to include the S3 prefix list destination routes to the S3 gateway endpoint.
- D. Update the S3 bucket policy to allow s3 PutObject access from the private subnet CIDR block.

**Answer: C**

**NEW QUESTION 43**

- (Exam Topic 1)

A company has an Amazon CloudFront distribution that uses an Amazon S3 bucket as its origin. During a review of the access logs, the company determines that some requests are going directly to the S3 bucket by using the website hosting endpoint. A SysOps administrator must secure the S3 bucket to allow requests only from CloudFront.

What should the SysOps administrator do to meet this requirement?

- A. Create an origin access identity (OAI) in CloudFront
- B. Associate the OAI with the distributio
- C. Remove access to and from other principals in the S3 bucket polic
- D. Update the S3 bucket policy to allow access only from the OAI.
- E. Create an origin access identity (OAI) in CloudFront
- F. Associate the OAI with the distributio
- G. Update the S3 bucket policy to allow access only from the OA
- H. Create a new origin, and specify the S3 bucket as the new origi
- I. Update the distribution behavior to use the new origi
- J. Remove the existing origin.
- K. Create an origin access identity (OAI) in CloudFront
- L. Associate the OAI with the distributio
- M. Update the S3 bucket policy to allow access only from the OA
- N. Disable website hostin
- O. Create a new origin, and specify the S3 bucket as the new origi
- P. Update the distribution behavior to use the new origi
- Q. Remove the existing origin.
- R. Update the S3 bucket policy to allow access only from the CloudFront distributio
- S. Remove access to and from other principals in the S3 bucket polic
- T. Disable website hostin
- . Create a new origin, and specify the S3 bucket as the new origi
- . Update the distribution behavior to use the new origi
- . Remove the existing origin.

**Answer: A**

**NEW QUESTION 46**

- (Exam Topic 1)

A Sysops administrator needs to configure automatic rotation for Amazon RDS database credentials. The credentials must rotate every 30 days. The solution must integrate with Amazon RDS.

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

- A. Store the credentials in AWS Systems Manager Parameter Store as a secure string
- B. Configure automatic rotation with a rotation interval of 30 days.
- C. Store the credentials in AWS Secrets Manager
- D. Configure automatic rotation with a rotation interval of 30 days.
- E. Store the credentials in a file in an Amazon S3 bucket
- F. Deploy an AWS Lambda function to automatically rotate the credentials every 30 days.
- G. Store the credentials in AWS Secrets Manager
- H. Deploy an AWS Lambda function to automatically rotate the credentials every 30 days.

**Answer:** B

**Explanation:**

Storing the credentials in AWS Secrets Manager and configuring automatic rotation with a rotation interval of 30 days is the most efficient way to meet the requirements with the least operational overhead. AWS Secrets Manager automatically rotates the credentials at the specified interval, so there is no need for an additional AWS Lambda function or manual rotation. Additionally, Secrets Manager is integrated with Amazon RDS, so the credentials can be easily used with the RDS database.

**NEW QUESTION 47**

- (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 50**

- (Exam Topic 1)

A new website will run on Amazon EC2 instances behind an Application Load Balancer. Amazon Route 53 will be used to manage DNS records.

What type of record should be set in Route 53 to point the website's apex domain name (for example company.com) to the Application Load Balancer?

- A. CNAME
- B. SOA
- C. TXT
- D. ALIAS

**Answer:** D

**NEW QUESTION 55**

- (Exam Topic 1)

A company uses an Amazon CloudFront distribution to deliver its website. Traffic logs for the website must be centrally stored, and all data must be encrypted at rest.

Which solution will meet these requirements?

- A. Create an Amazon OpenSearch Service (Amazon Elasticsearch Service) domain with internet access and server-side encryption that uses the default AWS managed key
- B. Configure CloudFront to use the Amazon OpenSearch Service (Amazon Elasticsearch Service) domain as a log destination.
- C. Create an Amazon OpenSearch Service (Amazon Elasticsearch Service) domain with VPC access and server-side encryption that uses AES-256. Configure CloudFront to use the Amazon OpenSearch Service (Amazon Elasticsearch Service) domain as a log destination.
- D. Create an Amazon S3 bucket that is configured with default server-side encryption that uses AES-256. Configure CloudFront to use the S3 bucket as a log destination.
- E. Create an Amazon S3 bucket that is configured with no default encryption
- F. Enable encryption in the CloudFront distribution, and use the S3 bucket as a log destination.

**Answer:** C

**NEW QUESTION 56**

- (Exam Topic 1)

A SysOps administrator must manage the security of an AWS account. Recently, an IAM user's access key was mistakenly uploaded to a public code repository. The SysOps administrator must identify anything that was changed by using this access key.

- A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to send all IAM events to an AWS Lambda function for analysis
- B. Query Amazon EC2 logs by using Amazon CloudWatch Logs Insights for all events related to the compromised access key within the suspected timeframe
- C. Search AWS CloudTrail event history for all events initiated with the compromised access key within the suspected timeframe
- D. Search VPC Flow Logs for all events initiated with the compromised access key within the suspected timeframe.

**Answer:** C

**NEW QUESTION 60**

- (Exam Topic 1)

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

**Answer:** A

**NEW QUESTION 61**



- (Exam Topic 1)

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
- B. Use the organization as the source. Retrieve the compliance data from the aggregator.
- C. Create an AWS Config aggregator in each account
- D. Use an S3 bucket in an aggregator account as the destination
- E. Retrieve the compliance data from the S3 bucket
- F. Edit the AWS Config policy in AWS Organization
- G. Use the organization's management account to turn on the s3-bucket-public-read-prohibited rule for the entire organization.
- H. Use the AWS Config compliance report from the organization's management account
- I. Filter the results by resource, and select Amazon S3.
- J. Use the AWS Config API to apply the s3-bucket-public-read-prohibited rule in all accounts for all available Regions.

**Answer:** CD

### NEW QUESTION 63

- (Exam Topic 1)

A company is storing backups in an Amazon S3 bucket. The backups must not be deleted for at least 3 months after the backups are created.

What should a SysOps administrator do to meet this requirement?

- A. Configure an IAM policy that denies the s3:DeleteObject action for all users
- B. Three months after an object is written, remove the policy.
- C. Enable S3 Object Lock on a new S3 bucket in compliance mode
- D. Place all backups in the new S3 bucket with a retention period of 3 months.
- E. Enable S3 Versioning on the existing S3 bucket
- F. Configure S3 Lifecycle rules to protect the backups.
- G. Enable S3 Object Lock on a new S3 bucket in governance mode
- H. Place all backups in the new S3 bucket with a retention period of 3 months.

**Answer:** D

#### Explanation:

To meet the requirements of the workload, a SysOps administrator should enable S3 Object Lock on a new S3 bucket in governance mode and place all backups in the new S3 bucket with a retention period of 3 months.

This will ensure that the backups are not deleted for at least 3 months after they are created. The other solutions (configuring an IAM policy that denies the s3:DeleteObject action for all users, enabling S3 Object Lock on a new S3 bucket in compliance mode, or enabling S3 Versioning on the existing S3 bucket and configuring S3 Lifecycle rules to protect the backups) will not meet the requirements, as they do not provide a way to ensure that the backups are not deleted for at least 3 months after they are created.

### NEW QUESTION 67

- (Exam Topic 1)

A company stores sensitive data in an Amazon S3 bucket. The company must log all access attempts to the S3 bucket. The company's risk team must receive immediate notification about any delete events.

Which solution will meet these requirements?

- A. Enable S3 server access logging for audit log
- B. Set up an Amazon Simple Notification Service (Amazon SNS) notification for the S3 bucket
- C. Select DeleteObject for the event type for the alert system.
- D. Enable S3 server access logging for audit log
- E. Launch an Amazon EC2 instance for the alert system. Run a cron job on the EC2 instance to download the access logs each day and to scan for a DeleteObject event.
- F. Use Amazon CloudWatch Logs for audit log
- G. Use Amazon CloudWatch alarms with an Amazon Simple Notification Service (Amazon SNS) notification for the alert system.
- H. Use Amazon CloudWatch Logs for audit log
- I. Launch an Amazon EC2 instance for the alert system. Run a cron job on the EC2 instance each day to compare the list of the items with the list from the previous day
- J. Configure the cron job to send a notification if an item is missing.

**Answer:** A

#### Explanation:

To meet the requirements of logging all access attempts to the S3 bucket and receiving immediate notification about any delete events, the company can enable S3 server access logging and set up an Amazon Simple Notification Service (Amazon SNS) notification for the S3 bucket. The S3 server access logs will record all access attempts to the bucket, including delete events, and the SNS notification can be configured to send an alert when a DeleteObject event occurs.

### NEW QUESTION 69

- (Exam Topic 1)

A SysOps administrator noticed that a large number of Elastic IP addresses are being created on the company's AWS account, but they are not being associated with Amazon EC2 instances, and are incurring Elastic IP address charges in the monthly bill.

How can the administrator identify who is creating the Elastic IP addresses?

- A. Attach a cost-allocation tag to each requested Elastic IP address with the IAM user name of the developer who creates it.
- B. Query AWS CloudTrail logs by using Amazon Athena to search for Elastic IP address events.
- C. Create a CloudWatch alarm on the EIPCreated metric and send an Amazon SNS notification when the alarm triggers.
- D. Use Amazon Inspector to get a report of all Elastic IP addresses created in the last 30 days.

**Answer:** B

#### NEW QUESTION 70

- (Exam Topic 1)

A company hosts its website on Amazon EC2 instances behind an Application Load Balancer. The company manages its DNS with Amazon Route 53. and wants to point its domain's zone apex to the website.

Which type of record should be used to meet these requirements?

- A. A CNAME record for the domain's zone apex
- B. An A record for the domain's zone apex
- C. An AAAA record for the domain's zone apex
- D. An alias record for the domain's zone apex

**Answer:** D

#### Explanation:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.htm>

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-elb-load-balancer.html>

#### NEW QUESTION 73

- (Exam Topic 1)

A company is undergoing an external audit of its systems, which run wholly on AWS. A SysOps administrator must supply documentation of Payment Card Industry Data Security Standard (PCI DSS) compliance for the infrastructure managed by AWS.

Which set of action should the SysOps administrator take to meet this requirement?

- A. Download the applicable reports from the AWS Artifact portal and supply these to the auditors.
- B. Download complete copies of the AWS CloudTrail log files and supply these to the auditors.
- C. Download complete copies of the AWS CloudWatch logs and supply these to the auditors.
- D. Provide the auditors with administrative access to the production AWS account so that the auditors can determine compliance.

**Answer:** A

#### NEW QUESTION 74

- (Exam Topic 1)

A company has a critical serverless application that uses multiple AWS Lambda functions. Each Lambda function generates 1 GB of log data daily in its own Amazon CloudWatch Logs log group. The company's security team asks for a count of application errors, grouped by type, across all of the log groups.

What should a SysOps administrator do to meet this requirement?

- A. Perform a CloudWatch Logs Insights query that uses the stats command and count function.
- B. Perform a CloudWatch Logs search that uses the groupby keyword and count function.
- C. Perform an Amazon Athena query that uses the SELECT and GROUP BY keywords.
- D. Perform an Amazon RDS query that uses the SELECT and GROUP BY keywords.

**Answer:** A

#### NEW QUESTION 78

- (Exam Topic 1)

A SysOps administrator is attempting to download patches from the internet into an instance in a private subnet. An internet gateway exists for the VPC, and a NAT gateway has been deployed on the public subnet; however, the instance has no internet connectivity. The resources deployed into the private subnet must be inaccessible directly from the public internet.

Public Subnet (10.0.1.0/24) Route Table	
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	IGW

  

Private Subnet (10.0.2.0/24) Route Table	
Destination	Target
10.0.0.0/16	local

What should be added to the private subnet's route table in order to address this issue, given the information provided?

- A. 0.0.0.0/0 IGW
- B. 0.0.0.0/0 NAT
- C. 10.0.1.0/24 IGW
- D. 10.0.1.0/24 NAT

**Answer:** B

#### NEW QUESTION 82

- (Exam Topic 1)

A SysOps Administrator runs a web application that is using a microservices approach whereby different responsibilities of the application have been divided in a separate microservice running on a different Amazon EC2 instance. The administrator has been tasked with reconfiguring the infrastructure to support this approach.

How can the administrator accomplish this with the LEAST administrative overhead?

- A. Use Amazon CloudFront to log the URL and forward the request.

- B. Use Amazon CloudFront to rewrite the header based on the microservice and forward the request.
- C. Use an Application Load Balancer (ALB) and do path-based routing.
- D. Use a Network Load Balancer (NLB) and do path-based routing.

**Answer:** C

**Explanation:**

<https://aws.amazon.com/premiumsupport/knowledge-center/elb-achieve-path-based-routing-alb/>

**NEW QUESTION 83**

- (Exam Topic 1)

A company runs hundreds of Amazon EC2 instances in a single AWS Region. Each EC2 instance has two attached 1 GiB General Purpose SSD (gp2) Amazon Elastic Block Store (Amazon EBS) volumes. A critical workload is using all the available IOPS capacity on the EBS volumes.

According to company policy, the company cannot change instance types or EBS volume types without completing lengthy acceptance tests to validate that the company's applications will function properly. A SysOps administrator needs to increase the I/O performance of the EBS volumes as quickly as possible.

Which action should the SysOps administrator take to meet these requirements?

- A. Increase the size of the 1 GiB EBS volumes.
- B. Add two additional elastic network interfaces on each EC2 instance.
- C. Turn on Transfer Acceleration on the EBS volumes in the Region.
- D. Add all the EC2 instances to a cluster placement group.

**Answer:** A

**Explanation:**

Increasing the size of the 1 GiB EBS volumes will increase the IOPS capacity of the volumes, which will improve the I/O performance of the EBS volumes. This option does not require any changes to the instance types or EBS volume types, so it can be done quickly without the need for lengthy acceptance tests to validate that the company's applications will function properly.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/requesting-ebs-volume-modifications.html>

**NEW QUESTION 86**

- (Exam Topic 1)

A company hosts an internal application on Amazon EC2 instances. All application data and requests route through an AWS Site-to-Site VPN connection between the on-premises network and AWS. The company must monitor the application for changes that allow network access outside of the corporate network. Any change that exposes the application externally must be restricted automatically.

Which solution meets these requirements in the MOST operationally efficient manner?

- A. Create an AWS Lambda function that updates security groups that are associated with the elastic network interface to remove inbound rules with noncorporate CIDR range
- B. Turn on VPC Flow Logs, and send the logs to Amazon CloudWatch Log
- C. Create an Amazon CloudWatch alarm that matches traffic from noncorporate CIDR ranges, and publish a message to an Amazon Simple Notification Service (Amazon SNS) topic with the Lambda function as a target.
- D. Create a scheduled Amazon EventBridge (Amazon CloudWatch Events) rule that targets an AWS Systems Manager Automation document to check for public IP addresses on the EC2 instance
- E. If public IP addresses are found on the EC2 instances, initiate another Systems Manager Automation document to terminate the instances.
- F. Configure AWS Config and a custom rule to monitor whether a security group allows inbound requests from noncorporate CIDR range
- G. Create an AWS Systems Manager Automation document to remove any noncorporate CIDR ranges from the application security groups.
- H. Configure AWS Config and the managed rule for monitoring public IP associations with the EC2 instances by ta
- I. Tag the EC2 instances with an identifier
- J. Create an AWS Systems Manager Automation document to remove the public IP association from the EC2 instances.

**Answer:** C

**Explanation:**

<https://aws.amazon.com/blogs/security/how-to-auto-remediate-internet-accessible-ports-with-aws-config-and-aw>

**NEW QUESTION 90**

- (Exam Topic 1)

A SysOps administrator is creating two AWS CloudFormation templates. The first template will create a VPC with associated resources, such as subnets, route tables, and an internet gateway. The second template will deploy application resources within the VPC that was created by the first template. The second template should refer to the resources created by the first template.

How can this be accomplished with the LEAST amount of administrative effort?

- A. Add an export field to the outputs of the first template and import the values in the second template.
- B. Create a custom resource that queries the stack created by the first template and retrieves the required values.
- C. Create a mapping in the first template that is referenced by the second template.
- D. Input the names of resources in the first template and refer to those names in the second template as a parameter.

**Answer:** A

**Explanation:**

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-stack-exports.html>

**NEW QUESTION 93**

- (Exam Topic 1)

A company is storing media content in an Amazon S3 bucket and uses Amazon CloudFront to distribute the content to its users. Due to licensing terms, the company is not authorized to distribute the content in some countries. A SysOps administrator must restrict access to certain countries.

What is the MOST operationally efficient solution that meets these requirements?



- A. Configure the S3 bucket policy to deny the GetObject operation based on the S3:LocationConstraint condition.
- B. Create a secondary origin access identity (OAI). Configure the S3 bucket policy to prevent access from unauthorized countries.
- C. Enable the geo restriction feature in the CloudFront distribution to prevent access from unauthorized countries.
- D. Update the application to generate signed CloudFront URLs only for IP addresses in authorized countries.

**Answer: C**

#### NEW QUESTION 94

- (Exam Topic 1)

A company is trying to connect two applications. One application runs in an on-premises data center that has a hostname of `host1.onprem.private`. The other application runs on an Amazon EC2 instance that has a hostname of `host1.awscloud.private`. An AWS Site-to-Site VPN connection is in place between the on-premises network and AWS.

The application that runs in the data center tries to connect to the application that runs on the EC2 instance, but DNS resolution fails. A SysOps administrator must implement DNS resolution between on-premises and AWS resources.

Which solution allows the on-premises application to resolve the EC2 instance hostname?

- A. Set up an Amazon Route 53 inbound resolver endpoint with a forwarding rule for the `onprem.private` hosted zone
- B. Associate the resolver with the VPC of the EC2 instance
- C. Configure the on-premises DNS resolver to forward `onprem.private` DNS queries to the inbound resolver endpoint.
- D. Set up an Amazon Route 53 inbound resolver endpoint
- E. Associate the resolver with the VPC of the EC2 instance
- F. Configure the on-premises DNS resolver to forward `awscloud.private` DNS queries to the inbound resolver endpoint.
- G. Set up an Amazon Route 53 outbound resolver endpoint with a forwarding rule for the `onprem.private` hosted zone
- H. Associate the resolver with the AWS Region of the EC2 instance
- I. Configure the on-premises DNS resolver to forward `onprem.private` DNS queries to the outbound resolver endpoint.
- J. Set up an Amazon Route 53 outbound resolver endpoint
- K. Associate the resolver with the AWS Region of the EC2 instance
- L. Configure the on-premises DNS resolver to forward `awscloud.private` DNS queries to the outbound resolver endpoint.

**Answer: C**

#### NEW QUESTION 95

- (Exam Topic 1)

A SysOps administrator needs to configure a solution that will deliver digital content to a set of authorized users through Amazon CloudFront. Unauthorized users must be restricted from access. Which solution will meet these requirements?

- A. Store the digital content in an Amazon S3 bucket that does not have public access blocked
- B. Use signed URLs to access the S3 bucket through CloudFront.
- C. Store the digital content in an Amazon S3 bucket that has public access blocked
- D. Use an origin access identity (OAI) to deliver the content through CloudFront
- E. Restrict S3 bucket access with signed URLs in CloudFront.
- F. Store the digital content in an Amazon S3 bucket that has public access blocked
- G. Use an origin access identity (OAI) to deliver the content through CloudFront
- H. Enable field-level encryption.
- I. Store the digital content in an Amazon S3 bucket that does not have public access blocked
- J. Use signed cookies for restricted delivery of the content through CloudFront.

**Answer: B**

#### NEW QUESTION 100

- (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 Synthetics canary
- G. Use the CloudWatch Synthetics Recorder plugin to generate the script for the canary run
- H. Configure the canary in line with requirement
- I. Create an alarm to provide alerts when issues are detected.

**Answer: A**

#### NEW QUESTION 105

- (Exam Topic 1)

A company has a mobile app that uses Amazon S3 to store images. The images are popular for a week, and then the number of access requests decreases over time. The images must be highly available and must be immediately accessible upon request. A SysOps administrator must reduce S3 storage costs for the company. Which solution will meet these requirements MOST cost-effectively?

- A. Create an S3 Lifecycle policy to transition the images to S3 Glacier after 7 days
- B. Create an S3 Lifecycle policy to transition the images to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 7 days
- C. Create an S3 Lifecycle policy to transition the images to S3 Standard after 7 days
- D. Create an S3 Lifecycle policy to transition the images to S3 Standard-Infrequent Access (S3 Standard-IA) after 7 days



**Answer:** D

#### NEW QUESTION 110

- (Exam Topic 1)

A SysOps administrator must configure a resilient tier of Amazon EC2 instances for a high performance computing (HPC) application. The HPC application requires minimum latency between nodes

Which actions should the SysOps administrator take to meet these requirements? (Select TWO.)

- A. Create an Amazon Elastic File System (Amazon EPS) file system Mount the file system to the EC2 instances by using user data
- B. Create a Multi-AZ Network Load Balancer in front of the EC2 instances
- C. Place the EC2 instances in an Auto Scaling group within a single subnet
- D. Launch the EC2 instances into a cluster placement group
- E. Launch the EC2 instances into a partition placement group

**Answer:** AD

#### NEW QUESTION 111

- (Exam Topic 1)

A SysOps administrator is maintaining a web application using an Amazon CloudFront web distribution, an Application Load Balancer (ALB), Amazon RDS, and Amazon EC2 in a VPC. All services have logging enabled. The administrator needs to investigate HTTP

Layer 7 status codes from the web application.

Which log sources contain the status codes? (Choose two.)

- A. VPC Flow Logs
- B. AWS CloudTrail logs
- C. ALB access logs
- D. CloudFront access logs
- E. RDS logs

**Answer:** CD

#### Explanation:

"C" because Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html>

"D" because "you can configure CloudFront to create log files that contain detailed information about every user request that CloudFront receives"

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html>

#### NEW QUESTION 116

- (Exam Topic 1)

A company uploaded its website files to an Amazon S3 bucket that has S3 Versioning enabled. The company uses an Amazon CloudFront distribution with the S3 bucket as the origin. The company recently modified the tiles, but the object names remained the same. Users report that old content is still appearing on the website.

How should a SysOps administrator remediate this issue?

- A. Create a CloudFront invalidation, and add the path of the updated files.
- B. Create a CloudFront signed URL to update each object immediately.
- C. Configure an S3 origin access identity (OAI) to display only the updated files to users.
- D. Disable S3 Versioning on the S3 bucket so that the updated files can replace the old files.

**Answer:** A

#### NEW QUESTION 121

- (Exam Topic 1)

A company is migrating its production file server to AWS. All data that is stored on the file server must remain accessible if an Availability Zone becomes unavailable or when system maintenance is performed. Users must be able to interact with the file server through the SMB protocol. Users also must have the ability to manage file permissions by using Windows ACLs.

Which solution will net these requirements?

- A. Create a single AWS Storage Gateway file gateway.
- B. Create an Amazon FSx for Windows File Server Multi-AZ file system.
- C. Deploy two AWS Storage Gateway file gateways across two Availability Zone
- D. Configure an Application Load Balancer in front of the file gateways.
- E. Deploy two Amazon FSx for Windows File Server Single-AZ 2 file system
- F. Configure Microsoft Distributed File System Replication (DFSR).

**Answer:** B

#### Explanation:

<https://aws.amazon.com/fsx/windows/>

#### NEW QUESTION 126

- (Exam Topic 1)

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 Shield Standard
- B. AWS WAF

- C. Elastic Load Balancing
- D. Amazon Cognito

**Answer:** B

#### NEW QUESTION 128

- (Exam Topic 1)

A company stores files on 50 Amazon S3 buckets in the same AWS Region. The company wants to connect to the S3 buckets securely over a private connection from its Amazon EC2 instances. The company needs a solution that produces no additional cost. Which solution will meet these requirements?

- A. Create a gateway VPC endpoint for each S3 bucket. Attach the gateway VPC endpoints to each subnet inside the VPC.
- B. Create an interface VPC endpoint for each S3 bucket. Attach the interface VPC endpoints to each subnet inside the VPC.
- C. Create one gateway VPC endpoint for all the S3 buckets. Add the gateway VPC endpoint to the VPC route table.
- D. Create one interface VPC endpoint for all the S3 buckets. Add the interface VPC endpoint to the VPC route table.

**Answer:** C

#### NEW QUESTION 130

- (Exam Topic 1)

A company hosts a web application on an Amazon EC2 instance. The web server logs are published to Amazon CloudWatch Logs. The log events have the same structure and include the HTTP response codes that are associated with the user requests. The company needs to monitor the number of times that the web server returns an HTTP 404 response.

What is the MOST operationally efficient solution that meets these requirements?

- A. Create a CloudWatch Logs metric filter that counts the number of times that the web server returns an HTTP 404 response.
- B. Create a CloudWatch Logs subscription filter that counts the number of times that the web server returns an HTTP 404 response.
- C. Create an AWS Lambda function that runs a CloudWatch Logs Insights query that counts the number of 404 codes in the log events during the past hour.
- D. Create a script that runs a CloudWatch Logs Insights query that counts the number of 404 codes in the log events during the past hour.

**Answer:** A

#### Explanation:

This is the most operationally efficient solution that meets the requirements, as it will allow the company to monitor the number of times that the web server returns an HTTP 404 response in real-time. The other solutions (creating a CloudWatch Logs subscription filter, an AWS Lambda function, or a script) will require additional steps and resources to monitor the number of times that the web server returns an HTTP 404 response.

A metric filter allows you to search for specific terms, phrases, or values in your log events, and then to create a metric based on the number of occurrences of those search terms. This allows you to create a CloudWatch Metric that can be used to create alarms and dashboards, which can be used to monitor the number of HTTP 404 responses returned by the web server.

#### NEW QUESTION 133

- (Exam Topic 1)

A company has a critical serverless application that uses multiple AWS Lambda functions. Each Lambda function generates 1 GB of log data daily in its own Amazon CloudWatch Logs log group. The company's security team asks for a count of application errors, grouped by type, across all of the log groups. What should a SysOps administrator do to meet this requirement?

- A. Perform a CloudWatch Logs Insights query that uses the stats command and count function.
- B. Perform a CloudWatch Logs search that uses the groupby keyword and count function.
- C. Perform an Amazon Athena query that uses the SELECT and GROUP BY keywords.
- D. Perform an Amazon RDS query that uses the SELECT and GROUP BY keywords.

**Answer:** A

#### NEW QUESTION 135

- (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 136

- (Exam Topic 1)

An ecommerce company uses an Amazon ElastiCache for Memcached cluster for in-memory caching of popular product queries on the shopping site. When viewing recent Amazon CloudWatch metrics data for the ElastiCache cluster, the SysOps administrator notices a large number of evictions. Which of the following actions will reduce these evictions? (Choose two.)

- A. Add an additional node to the ElastiCache cluster.
- B. Increase the ElastiCache time to live (TTL).
- C. Increase the individual node size inside the ElastiCache cluster.
- D. Put an Elastic Load Balancer in front of the ElastiCache cluster.
- E. Use Amazon Simple Queue Service (Amazon SQS) to decouple the ElastiCache cluster.

**Answer:** AC

**Explanation:**

<https://d1.awsstatic.com/training-and-certification/docs-sysops-associate/AWS-Certified-SysOps-Administrator>

#### NEW QUESTION 139

- (Exam Topic 1)

A company hosts several write-intensive applications. These applications use a MySQL database that runs on a single Amazon EC2 instance. The company asks a SysOps administrator to implement a highly available database solution that is ideal for multi-tenant workloads. Which solution should the SysOps administrator implement to meet these requirements?

- A. Create a second EC2 instance for MySQL
- B. Configure the second instance to be a read replica.
- C. Migrate the database to an Amazon Aurora DB cluster
- D. Add an Aurora Replica.
- E. Migrate the database to an Amazon Aurora multi-master DB cluster.
- F. Migrate the database to an Amazon RDS for MySQL DB instance.

**Answer:** C

#### NEW QUESTION 144

- (Exam Topic 1)

A company runs several workloads on AWS. The company identifies five AWS Trusted Advisor service quota metrics to monitor in a specific AWS Region. The company wants to receive email notification each time resource usage exceeds 60% of one of the service quotas. Which solution will meet these requirements?

- A. Create five Amazon CloudWatch alarms, one for each Trusted Advisor service quota metric
- B. Configure an Amazon Simple Notification Service (Amazon SNS) topic for email notification each time that usage exceeds 60% of one of the service quotas.
- C. Create five Amazon CloudWatch alarms, one for each Trusted Advisor service quota metric
- D. Configure an Amazon Simple Queue Service (Amazon SQS) queue for email notification each time that usage exceeds 60% of one of the service quotas.
- E. Use the AWS Service Health Dashboard to monitor each Trusted Advisor service quota metric. Configure an Amazon Simple Queue Service (Amazon SQS) queue for email notification each time that usage exceeds 60% of one of the service quotas.
- F. Use the AWS Service Health Dashboard to monitor each Trusted Advisor service quota metric. Configure an Amazon Simple Notification Service (Amazon SNS) topic for email notification each time that usage exceeds 60% of one of the service quotas.

**Answer:** A

**Explanation:**

CloudWatch alarms allow you to monitor AWS resources, and you can configure an SNS topic to send an email notification each time one of the alarms is triggered. This will ensure that the company receives email notifications each time one of the service quotas is exceeded, allowing the company to take action as needed.

#### NEW QUESTION 148

- (Exam Topic 1)

A company has multiple Amazon EC2 instances that run a resource-intensive application in a development environment. A SysOps administrator is implementing a solution to stop these EC2 instances when they are not in use. Which solution will meet this requirement?

- A. Assess AWS CloudTrail logs to verify that there is no EC2 API activity
- B. Invoke an AWS Lambda function to stop the EC2 instances.
- C. Create an Amazon CloudWatch alarm to stop the EC2 instances when the average CPU utilization is lower than 5% for a 30-minute period.
- D. Create an Amazon CloudWatch metric to stop the EC2 instances when the VolumeReadBytes metric is lower than 500 for a 30-minute period.
- E. Use AWS Config to invoke an AWS Lambda function to stop the EC2 instances based on resource configuration changes.

**Answer:** B

**Explanation:**

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/UsingAlarmActions.html#AddingStopAction>

#### NEW QUESTION 150

- (Exam Topic 1)

A SysOps administrator is creating an Amazon EC2 Auto Scaling group in a new AWS account. After adding some instances, the SysOps administrator notices that the group has not reached the minimum number of instances. The SysOps administrator receives the following error message:

```
Launching a new EC2 instance. Status Reason: Your quota allows for 0 more running instance(s).  
You requested at least 1. Launching EC2 instance failed.
```

Which action will resolve this issue?

- A. Adjust the account spending limits for Amazon EC2 on the AWS Billing and Cost Management console
- B. Modify the EC2 quota for that AWS Region in the EC2 Settings section of the EC2 console.
- C. Request a quota Increase for the Instance type family by using Service Quotas on the AWS Management Console.
- D. Use the Rebalance action In the Auto Scaling group on the AWS Management Console.

**Answer:** C

#### NEW QUESTION 155

- (Exam Topic 1)

A SysOps administrator Is troubleshooting an AWS Cloud Formation template whereby multiple Amazon EC2 instances are being created The template is working In us-east-1. but it is failing In us-west-2 with the error code:

```
AMI [ami-12345678] does not exist
```

How should the administrator ensure that the AWS Cloud Formation template is working in every region?

- A. Copy the source region's Amazon Machine Image (AMI) to the destination region and assign it the same ID.
- B. Edit the AWS CloudFormatton template to specify the region code as part of the fully qualified AMI ID.
- C. Edit the AWS CloudFormatton template to offer a drop-down list of all AMIs to the user by using the aws :: EC2:: ami :: imageID control.
- D. Modify the AWS CloudFormation template by including the AMI IDs in the "Mappings" sectio
- E. Refer to the proper mapping within the template for the proper AMI ID.

**Answer:** A

#### NEW QUESTION 158

- (Exam Topic 1)

A SysOps administrator is responsible for a legacy. CPU-heavy application The application can only be scaled vertically Currently, the application is deployed on a single t2 large Amazon EC2 instance The system is showing 90% CPU usage and significant performance latency after a few minutes What change should be made to alleviate the performance problem?

- A. Change the Amazon EBS volume to Provisioned IOPs
- B. Upgrade to a compute-optimized instance
- C. Add additional 12 large instances to the application
- D. Purchase Reserved Instances

**Answer:** B

#### NEW QUESTION 159

- (Exam Topic 1)

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 Replic
- B. Promote the replica to replace the primary DB instance.
- C. Create an AWS Lambda function to restore an automatic backup to the existing DB cluster.
- D. Use backtracking to rewind the existing DB cluster to the desired recovery point.
- E. Use point-in-time recovery to restore the existing DB cluster to the desired recovery point.

**Answer:** C

#### Explanation:

"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.Managing.Backtrack.html>

#### NEW QUESTION 164

- (Exam Topic 1)

A SysOps administrator launches an Amazon EC2 Linux instance in a public subnet. When the instance is running, the SysOps administrator obtains the public IP address and attempts to remotely connect to the instance multiple times. However, the SysOps administrator always receives a timeout error. Which action will allow the SysOps administrator to remotely connect to the instance?

- A. Add a route table entry in the public subnet for the SysOps administrator's IP address.
- B. Add an outbound network ACL rule to allow TCP port 22 for the SysOps administrator's IP address.
- C. Modify the instance security group to allow inbound SSH traffic from the SysOps administrator's IP address.
- D. Modify the instance security group to allow outbound SSH traffic to the SysOps administrator's IP address.

**Answer:** C

#### NEW QUESTION 168

- (Exam Topic 1)

An organization created an Amazon Elastic File System (Amazon EFS) volume with a file system ID of fs-85ba4Kc. and it is actively used by 10 Amazon EC2 hosts The organization has become concerned that the file system is not encrypted How can this be resolved?



- A. Enable encryption on each host's connection to the Amazon EFS volume Each connection must be recreated for encryption to take effect
- B. Enable encryption on the existing EFS volume by using the AWS Command Line Interface
- C. Enable encryption on each host's local drive Restart each host to encrypt the drive
- D. Enable encryption on a newly created volume and copy all data from the original volume Reconnect each host to the new volume

**Answer:** D

**Explanation:**

<https://docs.aws.amazon.com/efs/latest/ug/encryption.html>

Amazon EFS supports two forms of encryption for file systems, encryption of data in transit and encryption at rest. You can enable encryption of data at rest when creating an Amazon EFS file system. You can enable encryption of data in transit when you mount the file system.

**NEW QUESTION 171**

- (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 174**

- (Exam Topic 1)

A SysOps administrator notices a scale-up event for an Amazon EC2 Auto Scaling group Amazon CloudWatch shows a spike in the RequestCount metric for the associated Application Load Balancer The administrator would like to know the IP addresses for the source of the requests

Where can the administrator find this information?

- A. Auto Scaling logs
- B. AWS CloudTrail logs
- C. EC2 instance logs
- D. Elastic Load Balancer access logs

**Answer:** D

**Explanation:**

Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and troubleshoot issues.

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html>

**NEW QUESTION 175**

- (Exam Topic 1)

A SysOps administrator is setting up an automated process to recover an Amazon EC2 instance In the event of an underlying hardware failure. The recovered instance must have the same private IP address and the same Elastic IP address that the original instance had. The SysOps team must receive an email notification when the recovery process is initiated.

Which solution will meet these requirements?

- A. Create an Amazon CloudWatch alarm for the EC2 instance, and specify the StatusCheckFailedInstance metric
- B. Add an EC2 action to the alarm to recover the instance
- C. Add an alarm notification to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic
- D. Subscribe the SysOps team email address to the SNS topic.
- E. Create an Amazon CloudWatch alarm for the EC2 Instance, and specify the StatusCheckFailed\_System metric
- F. Add an EC2 action to the alarm to recover the instance
- G. Add an alarm notification to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic
- H. Subscribe the SysOps team email address to the SNS topic.
- I. Create an Auto Scaling group across three different subnets in the same Availability Zone with a minimum, maximum, and desired size of 1. Configure the Auto Scaling group to use a launch template that specifies the private IP address and the Elastic IP address
- J. Add an activity notification for the Auto Scaling group to send an email message to the SysOps team through Amazon Simple Email Service (Amazon SES).
- K. Create an Auto Scaling group across three Availability Zones with a minimum, maximum, and desired size of 1. Configure the Auto Scaling group to use a launch template that specifies the private IP address and the Elastic IP address
- L. Add an activity notification for the Auto Scaling group to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic
- M. Subscribe the SysOps team email address to the SNS topic.

**Answer:** B

**Explanation:**

You can create an Amazon CloudWatch alarm that monitors an Amazon EC2 instance and automatically recovers the instance if it becomes impaired due to an underlying hardware failure or a problem that requires AWS involvement to repair. Terminated instances cannot be recovered. A recovered instance is identical to the original instance, including the instance ID, private IP addresses, Elastic IP addresses, and all instance metadata. If the impaired instance has a public IPv4 address, the instance retains the public IPv4 address after recovery. If the impaired instance is in a placement group, the recovered instance runs in the placement group. When the StatusCheckFailed\_System alarm is triggered, and the recover action is initiated, you will be notified by the Amazon SNS topic that you selected when you created the alarm and associated the recover action. <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-recover.html>

**NEW QUESTION 177**

- (Exam Topic 1)

A SysOps administrator is troubleshooting connection timeouts to an Amazon EC2 instance that has a public IP address. The instance has a private IP address of 172.31.16.139. When the SysOps administrator tries to ping the instance's public IP address from the remote IP address 203.0.113.12, the response is "request timed out." The flow logs contain the following information:

```
2 123456789010 eni-1235b8ca123456789 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027 1432917142 ACCEPT OK
2 123456789010 eni-1235b8ca123456789 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094 1432917142 REJECT OK
```

What is one cause of the problem?

- A. Inbound security group deny rule
- B. Outbound security group deny rule
- C. Network ACL inbound rules
- D. Network ACL outbound rules

**Answer:** D

#### NEW QUESTION 178

- (Exam Topic 1)

A company uses AWS Organizations to manage multiple AWS accounts with consolidated billing enabled. Organization member account owners want the benefits of Reserved Instances (RIs) but do not want to share RIs with other accounts.

Which solution will meet these requirements?

- A. Purchase RIs in individual member account
- B. Disable RI discount sharing in the management account.
- C. Purchase RIs in individual member account
- D. Disable RI discount sharing in the member accounts.
- E. Purchase RIs in the management account
- F. Disable RI discount sharing in the management account.
- G. Purchase RIs in the management account
- H. Disable RI discount sharing in the member accounts.

**Answer:** A

#### Explanation:

<https://aws.amazon.com/premiumsupport/knowledge-center/ec2-ri-consolidated-billing/>

RI discounts apply to accounts in an organization's consolidated billing family depending upon whether RI sharing is turned on or off for the accounts. By default, RI sharing for all accounts in an organization is turned on. The management account of an organization can change this setting by turning off RI sharing for an account. The capacity reservation for an RI applies only to the account the RI was purchased on, no matter whether RI sharing is turned on or off.

#### NEW QUESTION 179

- (Exam Topic 1)

A company is running an application on premises and wants to use AWS for data backup. All of the data must be available locally. The backup application can write only to block-based storage that is compatible with the Portable Operating System Interface (POSIX).

Which backup solution will meet these requirements?

- A. Configure the backup software to use Amazon S3 as the target for the data backups
- B. Configure the backup software to use Amazon S3 Glacier as the target for the data backups
- C. Use AWS Storage Gateway, and configure it to use gateway-cached volumes
- D. Use AWS Storage Gateway, and configure it to use gateway-stored volumes

**Answer:** D

#### Explanation:

<https://docs.aws.amazon.com/storagegateway/latest/userguide/StorageGatewayConcepts.html>

#### NEW QUESTION 181

- (Exam Topic 1)

A company has an internal web application that runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group in a single Availability Zone.

A SysOps administrator must make the application highly available.

Which action should the SysOps administrator take to meet this requirement?

- A. Increase the maximum number of instances in the Auto Scaling group to meet the capacity that is required at peak usage.
- B. Increase the minimum number of instances in the Auto Scaling group to meet the capacity that is required at peak usage.
- C. Update the Auto Scaling group to launch new instances in a second Availability Zone in the same AWS Region.
- D. Update the Auto Scaling group to launch new instances in an Availability Zone in a second AWS Region.

**Answer:** C

#### NEW QUESTION 186

- (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 188

- (Exam Topic 1)

A company needs to implement a managed file system to host Windows file shares for users on premises. Resources in the AWS Cloud also need access to the data on these file shares. A SysOps administrator needs to present the user file shares on premises and make the user file shares available on AWS with minimum latency.

What should the SysOps administrator do to meet these requirements?

- A. Set up an Amazon S3 File Gateway.
- B. Set up an AWS Direct Connect connection.
- C. Use AWS DataSync to automate data transfers between the existing file servers and AWS.
- D. Set up an Amazon FSx File Gateway.

**Answer:** D

#### Explanation:

Amazon FSx provides a fully managed file system that is optimized for Windows-based workloads and can be used to create file shares that can be accessed both on premises and in the AWS Cloud. The file shares that are created in Amazon FSx are highly available and can be accessed with low latency. Additionally, Amazon FSx supports Windows-based authentication, making it easy to integrate with existing Windows user accounts.

References:

[1] <https://aws.amazon.com/fsx/>

[2] <https://aws.amazon.com/storage/file-storage/>

[3] <https://docs.aws.a>

#### NEW QUESTION 193

- (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 194

- (Exam Topic 1)

A global gaming company is preparing to launch a new game on AWS. The game runs in multiple AWS Regions on a fleet of Amazon EC2 instances. The instances are in an Auto Scaling group behind an

Application Load Balancer (ALB) in each Region. The company plans to use Amazon Route 53 for DNS services. The DNS configuration must direct users to the Region that is closest to them and must provide automated failover.

Which combination of steps should a SysOps administrator take to configure Route 53 to meet these requirements? (Select TWO.)

- A. Create Amazon CloudWatch alarms that monitor the health of the ALB in each Region. Configure Route 53 DNS failover by using a health check that monitors the alarms.
- B. Create Amazon CloudWatch alarms that monitor the health of the EC2 instances in each Region. Configure Route 53 DNS failover by using a health check that monitors the alarms.
- C. Configure Route 53 DNS failover by using a health check that monitors the private address of an EC2 instance in each Region.
- D. Configure Route 53 geoproximity routing. Specify the Regions that are used for the infrastructure.
- E. Configure Route 53 simple routing. Specify the continent, country, and state or province that are used for the infrastructure.

**Answer:** A

#### NEW QUESTION 199

- (Exam Topic 1)

A company has an existing web application that runs on two Amazon EC2 instances behind an Application Load Balancer (ALB) across two Availability Zones. The application uses an Amazon RDS Multi-AZ DB Instance. Amazon Route 53 record sets route requests for dynamic content to the load balancer and requests for static content to an Amazon S3 bucket. Site visitors are reporting extremely long loading times.

Which actions should be taken to improve the performance of the website? (Select TWO.)

- A. Add Amazon CloudFront caching for static content.
- B. Change the load balancer listener from HTTPS to TCP.
- C. Enable Amazon Route 53 latency-based routing.
- D. Implement Amazon EC2 Auto Scaling for the web servers.
- E. Move the static content from Amazon S3 to the web servers.

**Answer:** AD

#### NEW QUESTION 202

- (Exam Topic 1)

A SysOps administrator needs to develop a solution that provides email notification and inserts a record into a database every time a file is put into an Amazon S3 bucket.

What is the MOST operationally efficient solution that meets these requirements?

- A. Set up an S3 event notification that targets an Amazon Simple Notification Service (Amazon SNS) topic Create two subscriptions for the SNS topic Use one subscription to send the email notification Use the other subscription to invoke an AWS Lambda function that inserts the record into the database
- B. Set up an Amazon CloudWatch alarm that enters ALARM state whenever an object is created in the S3 bucket Configure the alarm to invoke an AWS Lambda function that sends the email notification and inserts the record into the database
- C. Create an AWS Lambda function to send the email notification and insert the record into the database whenever a new object is detected in the S3 bucket invoke the function every minute with an Amazon EventBridge (Amazon CloudWatch Events) scheduled rule.
- D. Set up two S3 event notifications Target a separate AWS Lambda function with each notification Configure one function to send the email notification Configure the other function to insert the record into the database

**Answer: C**

#### NEW QUESTION 207

- (Exam Topic 1)

A company runs a stateless application that is hosted on an Amazon EC2 instance. Users are reporting performance issues. A SysOps administrator reviews the Amazon CloudWatch metrics for the application and notices that the instance's CPU utilization frequently reaches 90% during business hours.

What is the MOST operationally efficient solution that will improve the application's responsiveness?

- A. Configure CloudWatch logging on the EC2 instance
- B. Configure a CloudWatch alarm for CPU utilization to alert the SysOps administrator when CPU utilization goes above 90%.
- C. Configure an AWS Client VPN connection to allow the application users to connect directly to the EC2 instance private IP address to reduce latency.
- D. Create an Auto Scaling group, and assign it to an Application Load Balance
- E. Configure a target tracking scaling policy that is based on the average CPU utilization of the Auto Scaling group.
- F. Create a CloudWatch alarm that activates when the EC2 instance's CPU utilization goes above 80%. Configure the alarm to invoke an AWS Lambda function that vertically scales the instance.

**Answer: C**

#### NEW QUESTION 212

- (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 Add an outbound deny rule for traffic to the external IP address
- E. Create a new security group to block traffic to the external IP address Assign the new security group to the entire VPC

**Answer: A**

#### NEW QUESTION 214

- (Exam Topic 1)

A company has multiple AWS Site-to-Site VPN connections between a VPC and its branch offices. The company manages an Amazon Elasticsearch Service (Amazon ES) domain that is configured with public access. The Amazon ES domain has an open domain access policy. A SysOps administrator needs to ensure that Amazon ES can be accessed only from the branch offices while preserving existing data.

Which solution will meet these requirements?

- A. Configure an identity-based access policy on Amazon ES
- B. Add an allow statement to the policy that includes the Amazon Resource Name (ARN) for each branch office VPN connection.
- C. Configure an IP-based domain access policy on Amazon ES
- D. Add an allow statement to the policy that includes the private IP CIDR blocks from each branch office network.
- E. Deploy a new Amazon ES domain in private subnets in a VPC, and import a snapshot from the old domain
- F. Create a security group that allows inbound traffic from the branch office CIDR blocks.
- G. Reconfigure the Amazon ES domain in private subnets in a VPC
- H. Create a security group that allows inbound traffic from the branch office CIDR blocks.

**Answer: B**

#### NEW QUESTION 215

- (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 Rekognition.
- C. Enable Amazon GuardDuty
- D. Configure S3 protection to monitor all data inside Amazon S3.
- E. Enable Amazon Macie
- 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 217**

- (Exam Topic 1)

A company website contains a web tier and a database tier on AWS. The web tier consists of Amazon EC2 instances that run in an Auto Scaling group across two Availability Zones. The database tier runs on an Amazon RDS for MySQL Multi-AZ DB instance. The database subnet network ACLs are restricted to only the web subnets that need access to the database. The web subnets use the default network ACL with the default rules.

The company's operations team has added a third subnet to the Auto Scaling group configuration. After an Auto Scaling event occurs, some users report that they intermittently receive an error message. The error message states that the server cannot connect to the database. The operations team has confirmed that the route tables are correct and that the required ports are open on all security groups.

Which combination of actions should a SysOps administrator take so that the web servers can communicate with the DB instance? (Select TWO.)

- A. On the default ACL
- B. create inbound Allow rules of type TCP with the ephemeral port range and the source as the database subnets.
- C. On the default ACL, create outbound Allow rules of type MySQL/Aurora (3306). Specify the destinations as the database subnets.
- D. On the network ACLs for the database subnets, create an inbound Allow rule of type MySQL/Aurora (3306). Specify the source as the third web subnet.
- E. On the network ACLs for the database subnets, create an outbound Allow rule of type TCP with the ephemeral port range and the destination as the third web subnet.
- F. On the network ACLs for the database subnets, create an outbound Allow rule of type MySQL/Aurora (3306). Specify the destination as the third web subnet.

**Answer:** CD

**NEW QUESTION 222**

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

**NEW QUESTION 225**

- (Exam Topic 1)

A company has a policy that requires all Amazon EC2 instances to have a specific set of tags. If an EC2 instance does not have the required tags, the noncompliant instance should be terminated.

What is the MOST operationally efficient solution that meets these requirements?

- A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to send all EC2 instance state changes to an AWS Lambda function to determine if each instance is compliant
- B. Terminate any noncompliant instances.
- C. Create an IAM policy that enforces all EC2 instance tag requirement
- D. If the required tags are not in place for an instance, the policy will terminate noncompliant instance.
- E. Create an AWS Lambda function to determine if each EC2 instance is compliant and terminate an instance if it is noncompliant
- F. Schedule the Lambda function to invoke every 5 minutes.
- G. Create an AWS Config rule to check if the required tags are present
- H. If an EC2 instance is noncompliant, invoke an AWS Systems Manager Automation document to terminate the instance.

**Answer:** D

**Explanation:**

<https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-automation.html>

**NEW QUESTION 226**

- (Exam Topic 1)

A company is rolling out a new version of its website. Management wants to deploy the new website in a limited rollout to 20% of the company's customers. The company uses Amazon Route 53 for its website's DNS solution.

Which configuration will meet these requirements?

- A. Create a failover routing policy
- B. Within the policy, configure 80% of the website traffic to be sent to the original resource
- C. Configure the remaining 20% of traffic as the failover record that points to the new resource.
- D. Create a multivalue answer routing policy

- E. Within the policy, create 4 records with the name and IP address of the original resource
- F. Configure 1 record with the name and IP address of the new resource.
- G. Create a latency-based routing policy
- H. Within the policy, configure a record pointing to the original resource with a weight of 80. Configure a record pointing to the new resource with a weight of 20.
- I. Create a weighted routing policy
- J. Within the policy, configure a weight of 80 for the record pointing to the original resource
- K. Configure a weight of 20 for the record pointing to the new resource.

**Answer:** C

#### NEW QUESTION 227

- (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 229

- (Exam Topic 1)

A company creates a new member account by using AWS Organizations. A SysOps administrator needs to add AWS Business Support to the new account. Which combination of steps must the SysOps administrator take to meet this requirement? (Select TWO.)

- A. Sign in to the new account by using 1AM credential
- B. Change the support plan.
- C. Sign in to the new account by using root user credential
- D. Change the support plan.
- E. Use the AWS Support API to change the support plan.
- F. Reset the password of the account root user.
- G. Create an IAM user that has administrator privileges in the new account.

**Answer:** BE

#### Explanation:

The best combination of steps to meet this requirement is to sign in to the new account by using root user credentials and change the support plan, and to create an IAM user that has administrator privileges in the new account.

Signing in to the new account by using root user credentials will allow the SysOps administrator to access the account and change the support plan to AWS Business Support. Additionally, creating an IAM user that has administrator privileges in the new account will ensure that the SysOps administrator has the necessary access to manage the account and make changes to the support plan if necessary.

Reference:

[1] [https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_accounts\\_access.html#orgs\\_ma](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_access.html#orgs_ma)

#### NEW QUESTION 230

- (Exam Topic 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.

**Answer:** A

**Explanation:**

Using Amazon S3 Block Public Access

as a centralized way to limit public access. Block Public Access

settings override bucket policies and object permissions. Be sure to enable Block Public Access for all accounts and buckets that you don't want publicly accessible.

<https://aws.amazon.com/premiumsupport/knowledge-center/secure-s3-resources/#:~:text=Using%20Amazon%2>

**NEW QUESTION 233**

- (Exam Topic 1)

A SysOps administrator needs to secure the credentials for an Amazon RDS database that is created by an AWS CloudFormation template. The solution must encrypt the credentials and must support automatic rotation.

Which solution will meet these requirements?

- A. Create an AWS::SecretsManager::Secret resource in the CloudFormation template
- B. Reference the credentials in the AWS::RDS::DBInstance resource by using the resolve:secretsmanager dynamic reference.
- C. Create an AWS::SecretsManager::Secret resource in the CloudFormation template
- D. Reference the credentials in the AWS::RDS::DBInstance resource by using the resolve:ssm-secure dynamic reference.
- E. Create an AWS::SSM::Parameter resource in the CloudFormation template
- F. Reference the credentials in the AWS::RDS::DBInstance resource by using the resolve:ssm dynamic reference.
- G. Create parameters for the database credentials in the CloudFormation template
- H. Use the Ref intrinsic function to provide the credentials to the AWS::RDS::DBInstance resource.

**Answer:** A

**NEW QUESTION 238**

- (Exam Topic 1)

A company has an application that is running on Amazon EC2 instances in a VPC. The application needs access to download software updates from the internet.

The VPC has public subnets and private subnets. The company's security policy requires all EC2 instances to be deployed in private subnets

What should a SysOps administrator do to meet those requirements?

- A. Add an internet gateway to the VPC In the route table for the private subnets, add a route to the internet gateway.
- B. Add a NAT gateway to a private subnet
- C. In the route table for the private subnets, add a route to the NAT gateway.
- D. Add a NAT gateway to a public subnet in the route table for the private subnets, add a route to the NAT gateway.
- E. Add two internet gateways to the VPC
- F. In the route table for the private subnets and public subnets, add a route to each internet gateway.

**Answer:** C

**NEW QUESTION 240**

- (Exam Topic 1)

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

**Answer:** D

**NEW QUESTION 243**

.....

## 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

### AWS-SysOps Practice Exam Features:

- \* AWS-SysOps Questions and Answers Updated Frequently
- \* AWS-SysOps Practice Questions Verified by Expert Senior Certified Staff
- \* AWS-SysOps Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* AWS-SysOps Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

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