

Exam Questions AWS-SysOps

Amazon AWS Certified SysOps Administrator - Associate

<https://www.2passeasy.com/dumps/AWS-SysOps/>



NEW QUESTION 1

- (Exam Topic 1)

A SysOps administrator has used AWS Cloud Formation to deploy a sereness application into a production VPC. The application consists of an AWS Lambda function, an Amazon DynamoDB table, and an Amazon API Gateway API. The SysOps administrator must delete the AWS Cloud Formation stack without deleting the DynamoDB table.

Which action should the SysOps administrator take before deleting the AWS Cloud Formation stack?

- A. Add a Retain deletion policy to the DynamoDB resource in the AWS CloudFormation stack.
- B. Add a Snapshot deletion policy to the DynamoDB resource In the AWS CloudFormation stack.
- C. Enable termination protection on the AWS Cloud Formation stack.
- D. Update the application's IAM policy with a Deny statement for the dynamodb:DeleteTable action.

Answer: A

NEW QUESTION 2

- (Exam Topic 1)

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

Which solution will meet this requirement?

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

Answer: C

Explanation:

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

NEW QUESTION 3

- (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 4

- (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 5

- (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 IAM 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

NEW QUESTION 6

- (Exam Topic 1)

A company runs a website from Sydney, Australia. Users in the United States (US) and Europe are reporting that images and videos are taking a long time to load. However, local testing in Australia indicates no performance issues. The website has a large amount of static content in the form of images and videos that are stored in Amazon S3.

Which solution will result in the MOST improvement in the user experience for users in the US and Europe?

- A. Configure AWS PrivateLink for Amazon S3.
- B. Configure S3 Transfer Acceleration.
- C. Create an Amazon CloudFront distribution.
- D. Distribute the static content to the CloudFront edge locations.
- E. Create an Amazon API Gateway API in each AWS Region.
- F. Cache the content locally.

Answer: D

NEW QUESTION 7

- (Exam Topic 1)

A SysOps administrator must set up notifications for whenever combined billing exceeds a certain threshold for all AWS accounts within a company. The administrator has set up AWS Organizations and enabled Consolidated Billing.

Which additional steps must the administrator perform to set up the billing alerts?

- A. In the payer account: Enable billing alerts in the Billing and Cost Management console; publish an Amazon SNS message when the billing alert triggers.
- B. In each account: Enable billing alerts in the Billing and Cost Management console; set up a billing alarm in Amazon CloudWatch; publish an SNS message when the alarm triggers.
- C. In the payer account: Enable billing alerts in the Billing and Cost Management console; set up a billing alarm in the Billing and Cost Management console to publish an SNS message when the alarm triggers.
- D. In the payer account: Enable billing alerts in the Billing and Cost Management console; set up a billing alarm in Amazon CloudWatch; publish an SNS message when the alarm triggers.

Answer: D

NEW QUESTION 8

- (Exam Topic 1)

A SysOps administrator is provisioning an Amazon Elastic File System (Amazon EFS) file system to provide shared storage across multiple Amazon EC2 instances. The instances all exist in the same VPC across multiple Availability Zones. There are two instances in each Availability Zone. The SysOps administrator must make the file system accessible to each instance with the lowest possible latency.

Which solution will meet these requirements?

- A. Create a mount target for the EFS file system in the VPC.
- B. Use the mount target to mount the file system on each of the instances.
- C. Create a mount target for the EFS file system in one Availability Zone of the VPC.
- D. Use the mount target to mount the file system on the instances in that Availability Zone.
- E. Share the directory with the other instances.
- F. Create a mount target for each instance.
- G. Use each mount target to mount the EFS file system on each respective instance.
- H. Create a mount target in each Availability Zone of the VPC. Use the mount target to mount the EFS file system on the instances in the respective Availability Zone.

Answer: D

Explanation:

A mount target provides an IP address for an NFSv4 endpoint at which you can mount an Amazon EFS file system. You mount your file system using its Domain Name Service (DNS) name, which resolves to the IP address of the EFS mount target in the same Availability Zone as your EC2 instance. You can create one mount target in each Availability Zone in an AWS Region. If there are multiple subnets in an Availability Zone in your VPC, you create a mount target in one of the subnets. Then all EC2 instances in that Availability Zone share that mount target. <https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html>

NEW QUESTION 9

- (Exam Topic 1)

An application team uses an Amazon Aurora MySQL DB cluster with one Aurora Replica. The application team notices that the application read performance degrades when user connections exceed 200. The number of user connections is typically consistent around 180, with occasional sudden increases above 200 connections. The application team wants the application to automatically scale as user demand increases or decreases.

Which solution will meet these requirements?

- A. Migrate to a new Aurora multi-master DB cluster.
- B. Modify the application database connection string.
- C. Modify the DB cluster by changing to serverless mode whenever user connections exceed 200.
- D. Create an auto scaling policy with a target metric of 195 DatabaseConnections.
- E. Modify the DB cluster by increasing the Aurora Replica instance size.

Answer: C

NEW QUESTION 10

- (Exam Topic 1)

A company has created a NAT gateway in a public subnet in a VPC. The VPC also contains a private subnet that includes Amazon EC2 instances. The EC2 instances use the NAT gateway to access the internet to download patches and updates. The company has configured a VPC flow log for the elastic network interface of the NAT gateway. The company is publishing the output to Amazon CloudWatch Logs.

A SysOps administrator must identify the top five internet destinations that the EC2 instances in the private subnet communicate with for downloads.

What should the SysOps administrator do to meet this requirement in the MOST operationally efficient way?

- A. Use AWS CloudTrail Insights events to identify the top five internet destinations.
- B. Use Amazon CloudFront standard logs (access logs) to identify the top five internet destinations.
- C. Use CloudWatch Logs Insights to identify the top five internet destinations.
- D. Change the flow log to publish logs to Amazon S3. Use Amazon Athena to query the log files in Amazon S3.

Answer: C

NEW QUESTION 10

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

Answer: B

Explanation:

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

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

NEW QUESTION 13

- (Exam Topic 1)

A company stores its data in an Amazon S3 bucket. The company is required to classify the data and find any sensitive personal information in its S3 files.

Which solution will meet these requirements?

- A. Create an AWS Config rule to discover sensitive personal information in the S3 files and mark them as noncompliant.
- B. Create an S3 event-driven artificial intelligence/machine learning (AI/ML) pipeline to classify sensitive personal information by using Amazon Recognition.
- C. Enable Amazon 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 17

- (Exam Topic 1)

A SysOps administrator must create a solution that immediately notifies software developers if an AWS Lambda function experiences an error.

Which solution will meet this requirement?

- A. Create an Amazon Simple Notification Service (Amazon SNS) topic with an email subscription for each developer.
- B. Create an Amazon CloudWatch alarm by using the Errors metric and the Lambda function name as a dimension.
- C. Configure the alarm to send a notification to the SNS topic when the alarm state reaches ALARM.
- D. Create an Amazon Simple Notification Service (Amazon SNS) topic with a mobile subscription for each developer.
- E. Create an Amazon EventBridge (Amazon CloudWatch Events) alarm by using LambdaError as the event pattern and the SNS topic name as a resource.
- F. Configure the alarm to send a notification to the SNS topic when the alarm state reaches ALARM.
- G. Verify each developer email address in Amazon Simple Email Service (Amazon SES). Create an Amazon CloudWatch rule by using the LambdaError metric and developer email addresses as dimension.
- H. Configure the rule to send an email through Amazon SES when the rule state reaches ALARM.

- I. Verify each developer mobile phone in Amazon Simple Email Service (Amazon SES). Create an Amazon EventBridge (Amazon CloudWatch Events) rule by using Errors as the event pattern and the Lambda function name as a resource.
- J. Configure the rule to send a push notification through Amazon SES when the rule state reaches ALARM.

Answer: A

NEW QUESTION 20

- (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 22

- (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 27

- (Exam Topic 1)

A company is partnering with an external vendor to provide data processing services. For this integration, the vendor must host the company's data in an Amazon S3 bucket in the vendor's AWS account. The vendor is allowing the company to provide an AWS Key Management Service (AWS KMS) key to encrypt the company's data. The vendor has provided an IAM role Amazon Resource Name (ARN) to the company for this integration. What should a SysOps administrator do to configure this integration?

- A. Create a new KMS key
- B. Add the vendor's IAM role ARN to the KMS key policy
- C. Provide the new KMS key ARN to the vendor.
- D. Create a new KMS key
- E. Create a new IAM user
- F. Add the vendor's IAM role ARN to an inline policy that is attached to the IAM user
- G. Provide the new IAM user ARN to the vendor.
- H. Configure encryption using the KMS managed S3 key
- I. Add the vendor's IAM role ARN to the KMS managed S3 key policy
- J. Provide the KMS managed S3 key ARN to the vendor.
- K. Configure encryption using the KMS managed S3 key
- L. Create an S3 bucket
- M. Add the vendor's IAM role ARN to the S3 bucket policy
- N. Provide the S3 bucket ARN to the vendor.

Answer: C

NEW QUESTION 32

- (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 36

- (Exam Topic 1)

A company has two VPC networks named VPC A and VPC B. The VPC A CIDR block is 10.0.0.0/16 and the VPC B CIDR block is 172.31.0.0/16. The company wants to establish a VPC peering connection named pcx-12345 between both VPCs.

Which rules should appear in the route table of VPC A after configuration? (Select TWO.)

- A. Destination: 10.0.0.0/16, Target: Local
- B. Destination: 172.31.0.0/16, Target: Local
- C. Destination: 10.0.0.0/16, Target: pcx-12345
- D. Destination: 172.31.0.0/16, Target: pcx-12345
- E. Destination: 10.0.0.0/16, Target: 172.31.0.0/16

Answer: AD

Explanation:

<https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-routing.html>

NEW QUESTION 38

- (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 40

- (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 43

- (Exam Topic 1)

A SysOps administrator has created a VPC that contains a public subnet and a private subnet. Amazon EC2 instances that were launched in the private subnet cannot access the internet. The default network ACL is active on all subnets in the VPC, and all security groups allow all outbound traffic:

Which solution will provide the EC2 instances in the private subnet with access to the internet?

- A. Create a NAT gateway in the public subnet.
- B. Create a route from the private subnet to the NAT gateway.
- C. Create a NAT gateway in the private subnet.
- D. Create a route from the public subnet to the NAT gateway.
- E. Create a NAT gateway in the private subnet.
- F. Create a route from the public subnet to the NAT gateway.
- G. Create a NAT gateway in the public subnet.
- H. Create a route from the private subnet to the NAT gateway.

Answer: A

Explanation:

NAT Gateway resides in public subnet, and traffic should be routed from private subnet to NAT Gateway: <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>

NEW QUESTION 48

- (Exam Topic 1)

A company wants to create an automated solution for all accounts managed by AWS Organizations to detect any security groups that have 0.0.0.0/0 as the source address for inbound traffic. The company also wants to automatically remediate any noncompliant security groups by restricting access to a specific CIDR block that corresponds with the company's intranet.

- A. Create an AWS Config rule to detect noncompliant security groups
- B. Set up automatic remediation to change the 0.0.0.0/0 source address to the approved CIDR block.
- C. Create an IAM policy to deny the creation of security groups that have 0.0.0.0/0 as the source address. Attach this IAM policy to every user in the company.
- D. Create an AWS Lambda function to inspect new and existing security groups, check for a noncompliant 0.0.0.0/0 source address, and change the source address to the approved CIDR block.
- E. Create a service control policy (SCP) for the organizational unit (OU) to deny the creation of security groups that have the 0.0.0.0/0 source address.
- F. Set up automatic remediation to change the 0.0.0.0/0 source address to the approved CIDR block.

Answer: A

NEW QUESTION 52

- (Exam Topic 1)

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 56

- (Exam Topic 1)

A gaming application is deployed on four Amazon EC2 instances in a default VPC. The SysOps administrator has noticed consistently high latency in responses as data is transferred among the four instances. There is no way for the administrator to alter the application code.

The MOST effective way to reduce latency is to relaunch the EC2 instances in:

- A. a dedicated VPC.
- B. a single subnet inside the VPC.
- C. a placement group.
- D. a single Availability Zone.

Answer: C

NEW QUESTION 60

- (Exam Topic 1)

A company is hosting applications on Amazon EC2 instances. The company is hosting a database on an Amazon RDS for PostgreSQL DB instance. The company requires all connections to the DB instance to be encrypted.

What should a SysOps administrator do to meet this requirement?

- A. Allow SSL connections to the database by using an inbound security group rule.
- B. Encrypt the database by using an AWS Key Management Service (AWS KMS) encryption key.
- C. Enforce SSL connections to the database by using a custom parameter group.
- D. Patch the database with SSL/TLS by using a custom PostgreSQL extension.

Answer: C

Explanation:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/PostgreSQL.Concepts.General.SSL.htm> Amazon RDS supports SSL/TLS encryption for connections to the database, and this can be enabled by creating a custom parameter group and setting the `rds.force_ssl` parameter to 1. This will ensure that all connections to the database are encrypted, protecting the data and maintaining compliance with the company's requirements.

NEW QUESTION 62

- (Exam Topic 1)

A company runs a web application on three Amazon EC2 instances behind an Application Load Balancer (ALB). The company notices that random periods of increased traffic cause a degradation in the application's performance. A SysOps administrator must scale the application to meet the increased traffic.

Which solution meets these requirements?

- A. Create an Amazon CloudWatch alarm to monitor application latency and increase the size of each EC2 instance if the desired threshold is reached.
- B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to monitor application latency and add an EC2 instance to the ALB if the desired threshold is reached.

reached.

- C. Deploy the application to an Auto Scaling group of EC2 instances with a target tracking scaling policy. Attach the ALB to the Auto Scaling group.
- D. Deploy the application to an Auto Scaling group of EC2 instances with a scheduled scaling policy. Attach the ALB to the Auto Scaling group.

Answer: C

Explanation:

docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html

NEW QUESTION 64

- (Exam Topic 1)

A company is attempting to manage its costs in the AWS Cloud. A SysOps administrator needs specific company-defined tags that are assigned to resources to appear on the billing report.

What should the SysOps administrator do to meet this requirement?

- A. Activate the tags as AWS generated cost allocation tags.
- B. Activate the tags as user-defined cost allocation tags.
- C. Create a new cost category
- D. Select the account billing dimension.
- E. Create a new AWS Cost and Usage Report
- F. Include the resource IDs.

Answer: B

Explanation:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/custom-tags.html> "User-defined tags are tags that you define, create, and apply to resources. After you have created and applied the user-defined tags, you can activate by using the Billing and Cost Management console for cost allocation tracking. "

To meet this requirement, the SysOps administrator should activate the company-defined tags as user-defined cost allocation tags. This will ensure that the tags appear on the billing report and that the resources can be tracked with the specific tags. The other options (activating the tags as AWS generated cost allocation tags, creating a new cost category and selecting the account billing dimension, and creating a new AWS Cost and Usage Report and including the resource IDs) will not meet the requirements and are not the correct solutions for this issue.

NEW QUESTION 69

- (Exam Topic 1)

A company's web application is available through an Amazon CloudFront distribution and directly through an internet-facing Application Load Balancer (ALB). A SysOps administrator must make the application accessible only through the CloudFront distribution and not directly through the ALB. The SysOps administrator must make this change without changing the application code. Which solution will meet these requirements?

- A. Modify the ALB type to internal. Set the distribution's origin to the internal ALB domain name.
- B. Create a Lambda@Edge function. Configure the function to compare a custom header value in the request with a stored password and to forward the request to the origin in case of a match. Associate the function with the distribution.
- C. Replace the ALB with a new internal ALB. Set the distribution's origin to the internal ALB domain name. Add a custom HTTP header to the origin settings for the distribution. In the ALB listener, add a rule to forward requests that contain the matching custom header and the header's value. Add a default rule to return a fixed response code of 403.
- D. Add a custom HTTP header to the origin settings for the distribution. In the ALB listener, add a rule to forward requests that contain the matching custom header and the header's value. Add a default rule to return a fixed response code of 403.

Answer: D

Explanation:

To make the application accessible only through the CloudFront distribution and not directly through the Application Load Balancer (ALB), you can add a custom HTTP header to the origin settings for the CloudFront distribution. You can then create a rule in the ALB listener to forward requests that contain the matching custom header and its value to the origin. You can also add a default rule to the ALB listener to return a fixed response code of 403 for requests that do not contain the matching custom header. This will allow you to redirect all requests to the CloudFront distribution and block direct access to the application through the ALB. <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/restrict-access-to-load-balancer.html>

NEW QUESTION 74

- (Exam Topic 1)

A SysOps administrator created an Amazon VPC with an IPv6 CIDR block, which requires access to the internet. However, access from the internet towards the VPC is prohibited. After adding and configuring the required components to the VPC, the administrator is unable to connect to any of the domains that reside on the internet.

What additional route destination rule should the administrator add to the route tables?

- A. Route `::/0` traffic to a NAT gateway
- B. Route `::/0` traffic to an internet gateway
- C. Route `0.0.0.0/0` traffic to an egress-only internet gateway
- D. Route `::/0` traffic to an egress-only internet gateway

Answer: D

Explanation:

<https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html>

NEW QUESTION 79

- (Exam Topic 1)

A SysOps administrator is tasked with analyzing database performance. The database runs on a single Amazon RDS D6 instance. The SysOps administrator finds that, during times of peak traffic, resources on the database are over utilized due to the amount of read traffic.

Which actions should the SysOps administrator take to improve RDS performance? (Select TWO.)

- A. Add a read replica.
- B. Modify the application to use Amazon ElastiCache for Memcached.
- C. Migrate the database from RDS to Amazon DynamoDB.
- D. Migrate the database to Amazon EC2 with enhanced networking enabled
- E. Upgrade the database to a Multi-AZ deployment.

Answer: AB

NEW QUESTION 83

- (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 88

- (Exam Topic 1)

A SysOps administrator is unable to authenticate an AWS CLI call to an AWS service Which of the following is the cause of this issue?

- A. The IAM password is incorrect
- B. The server certificate is missing
- C. The SSH key pair is incorrect
- D. There is no access key

Answer: C

NEW QUESTION 91

- (Exam Topic 1)

A company has an AWS Cloud Formation template that creates an Amazon S3 bucket. A user authenticates to the corporate AWS account with their Active Directory credentials and attempts to deploy the Cloud Formation template. However, the stack creation fails. Which factors could cause this failure? (Select TWO.)

- A. The user's IAM policy does not allow the cloudformation:CreateStack action.
- B. The user's IAM policy does not allow the cloudformation:CreateStackSet action.
- C. The user's IAM policy does not allow the s3:CreateBucket action.
- D. The user's IAM policy explicitly denies the s3:ListBucket action.
- E. The user's IAM policy explicitly denies the s3:PutObject action

Answer: AC

NEW QUESTION 95

- (Exam Topic 1)

A company's reporting job that used to run in 15 minutes is now taking an hour to run. An application generates the reports. The application runs on Amazon EC2 instances and extracts data from an Amazon RDS for MySQL database. A SysOps administrator checks the Amazon CloudWatch dashboard for the RDS instance and notices that the Read IOPS metrics are high, even when the reports are not running. The SysOps administrator needs to improve the performance and the availability of the RDS instance. Which solution will meet these requirements?

- A. Configure an Amazon ElastiCache cluster in front of the RDS instance
- B. Update the reporting job to query the ElastiCache cluster.
- C. Deploy an RDS read replica
- D. Update the reporting job to query the reader endpoint.
- E. Create an Amazon CloudFront distribution
- F. Set the RDS instance as the origin
- G. Update the reporting job to query the CloudFront distribution.
- H. Increase the size of the RDS instance.

Answer: B

Explanation:

Using an RDS read replica will improve the performance and availability of the RDS instance by offloading read queries to the replica. This will also ensure that the reporting job completes in a timely manner and does not affect the performance of other queries that might be running on the RDS instance. Additionally, updating the reporting job to query the reader endpoint will ensure that all read queries are directed to the read replica.

Reference: [1] https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

NEW QUESTION 98

- (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 103

- (Exam Topic 1)

A large company is using AWS Organizations to manage its multi-account AWS environment. According to company policy, all users should have read-level access to a particular Amazon S3 bucket in a central account. The S3 bucket data should not be available outside the organization. A SysOps administrator must set up the permissions and add a bucket policy to the S3 bucket.

Which parameters should be specified to accomplish this in the MOST efficient manner?

- A. Specify "" as the principal and PrincipalOrgId as a condition.
- B. Specify all account numbers as the principal.
- C. Specify PrincipalOrgId as the principal.
- D. Specify the organization's management account as the principal.

Answer: A

Explanation:

<https://aws.amazon.com/blogs/security/control-access-to-aws-resources-by-using-the-aws-organization-of-iam-p>

NEW QUESTION 106

- (Exam Topic 1)

A company must ensure that any objects uploaded to an S3 bucket are encrypted. Which of the following actions will meet this requirement? (Choose two.)

- A. Implement AWS Shield to protect against unencrypted objects stored in S3 buckets.
- B. Implement Object access control list (ACL) to deny unencrypted objects from being uploaded to the S3 bucket.
- C. Implement Amazon S3 default encryption to make sure that any object being uploaded is encrypted before it is stored.
- D. Implement Amazon Inspector to inspect objects uploaded to the S3 bucket to make sure that they are encrypted.
- E. Implement S3 bucket policies to deny unencrypted objects from being uploaded to the buckets.

Answer: CE

Explanation:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/default-bucket-encryption.html>

You can set the default encryption behavior on an Amazon S3 bucket so that all objects are encrypted when they are stored in the bucket. The objects are encrypted using server-side encryption with either Amazon S3-managed keys (SSE-S3) or AWS Key Management Service (AWS KMS) customer master keys (CMKs).

<https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/> How to Prevent Uploads of Unencrypted Objects to Amazon S3#

By using an S3 bucket policy, you can enforce the encryption requirement when users upload objects, instead of assigning a restrictive IAM policy to all users.

NEW QUESTION 109

- (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#AddingStopActi>

NEW QUESTION 113

- (Exam Topic 1)

A company has an Amazon RDS DB instance. The company wants to implement a caching service while maintaining high availability.

Which combination of actions will meet these requirements? (Choose two.)

- A. Add Auto Discovery to the data store.
- B. Create an Amazon ElastiCache for Memcached data store.
- C. Create an Amazon ElastiCache for Redis data store.
- D. Enable Multi-AZ for the data store.
- E. Enable Multi-threading for the data store.

Answer: CD

Explanation:

<https://aws.amazon.com/elasticache/memcached/> <https://aws.amazon.com/elasticache/redis/>

NEW QUESTION 118

- (Exam Topic 1)

A company asks a SysOps administrator to ensure that AWS CloudTrail files are not tampered with after they are created. Currently, the company uses AWS Identity and Access Management (IAM) to restrict access to specific trails. The company's security team needs the ability to trace the integrity of each file. What is the MOST operationally efficient solution that meets these requirements?

- A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function when a new file is delivered
- B. Configure the Lambda function to compute an MD5 hash check on the file and store the result in an Amazon DynamoDB table
- C. The security team can use the values that are stored in DynamoDB to verify the integrity of the delivered files.
- D. Create an AWS Lambda function that is invoked each time a new file is delivered to the CloudTrail bucket
- E. Configure the Lambda function to compute an MD5 hash check on the file and store the result as a tag in an Amazon S3 object
- F. The security team can use the information in the tag to verify the integrity of the delivered files.
- G. Enable the CloudTrail file integrity feature on an Amazon S3 bucket
- H. Create an IAM policy that grants the security team access to the file integrity logs that are stored in the S3 bucket.
- I. Enable the CloudTrail file integrity feature on the trail
- J. The security team can use the digest file that is created by CloudTrail to verify the integrity of the delivered files.

Answer: D

Explanation:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html> "When you enable log file integrity validation, CloudTrail creates a hash for every log file that it delivers.

Every hour, CloudTrail also creates and delivers a file that references the log files for the last hour and contains a hash of each. This file is called a digest file. Validated log files are invaluable in security and forensic investigations"

NEW QUESTION 121

- (Exam Topic 1)

A user working in the Amazon EC2 console increased the size of an Amazon Elastic Block Store (Amazon EBS) volume attached to an Amazon EC2 Windows instance. The change is not reflected in the file system. What should a SysOps administrator do to resolve this issue?

- A. Extend the file system with operating system-level tools to use the new storage capacity.
- B. Reattach the EBS volume to the EC2 instance.
- C. Reboot the EC2 instance that is attached to the EBS volume.
- D. Take a snapshot of the EBS volume
- E. Replace the original volume with a volume that is created from the snapshot.

Answer: B

NEW QUESTION 122

- (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 124

- (Exam Topic 1)

A company has deployed a web application in a VPC that has subnets in three Availability Zones. The company launches three Amazon EC2 instances from an EC2 Auto Scaling group behind an Application Load Balancer (ALB).

A SysOps administrator notices that two of the EC2 instances are in the same Availability Zone, rather than being distributed evenly across all three Availability Zones. There are no errors in the Auto Scaling group's activity history.

What is the MOST likely reason for the unexpected placement of EC2 instances?

- A. One Availability Zone did not have sufficient capacity for the requested EC2 instance type.
- B. The ALB was configured for only two Availability Zones.
- C. The Auto Scaling group was configured for only two Availability Zones.
- D. Amazon EC2 Auto Scaling randomly placed the instances in Availability Zones.

Answer: C

Explanation:

the autoscaling group is responsible to add the instances in the subnets

NEW QUESTION 126

- (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 128

- (Exam Topic 1)

A company's application currently uses an IAM role that allows all access to all AWS services. A SysOps administrator must ensure that the company's IAM policies allow only the permissions that the application requires.

How can the SysOps administrator create a policy to meet this requirement?

- A. Turn on AWS CloudTrail
- B. Generate a policy by using AWS Security Hub.
- C. Turn on Amazon EventBridge (Amazon CloudWatch Events). Generate a policy by using AWS Identity and Access Management Access Analyzer.
- D. Use the AWS CLI to run the get-generated-policy command in AWS Identity and Access Management Access Analyzer.
- E. Turn on AWS CloudTrail
- F. Generate a policy by using AWS Identity and Access Management Access Analyzer.

Answer: D

Explanation:

Generate a policy by using AWS Identity and Access Management Access Analyzer. AWS CloudTrail is a service that records all API calls made on your account. You can use this data to generate a policy with AWS Identity and Access Management Access Analyzer that only allows the permissions that the application requires. This will ensure that the application only has the necessary permissions and will protect the company from any unauthorized access.

<https://docs.aws.amazon.com/IAM/latest/UserGuide/what-is-access-analyzer.html#what-is-access-analyzer-poli>

NEW QUESTION 132

- (Exam Topic 1)

A Sysops administrator has created an Amazon EC2 instance using an AWS CloudFormation template in the us-east-1 Region. The administrator finds that this template has failed to create an EC2 instance in the us-west-2 Region. What is one cause for this failure?

- A. Resource tags defined in the CloudFormation template are specific to the us-east-1 Region.
- B. The Amazon Machine Image (AMI) ID referenced in the CloudFormation template could not be found in the us-west-2 Region.
- C. The cfn-init script did not run during resource provisioning in the us-west-2 Region.
- D. The IAM user was not created in the specified Region.

Answer: B

Explanation:

One possible cause for the failure of the CloudFormation template to create an EC2 instance in the us-west-2 Region is that the Amazon Machine Image (AMI) ID referenced in the template could not be found in the us-west-2 Region. This could be due to the fact that the AMI is not available in that region, or the credentials used to access the AMI were not configured properly. The other options (resource tags defined in the CloudFormation template are specific to the us-east-1 Region, the cfn-init script did not run during resource provisioning in the us-west-2 Region, and the IAM user was not created in the specified Region) are not valid causes for this failure.

NEW QUESTION 134

- (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 SysOps administrator needs to delete an AWS CloudFormation stack that is no longer in use. The CloudFormation stack is in the DELETE_FAILED state. The SysOps administrator has validated the permissions that are required to delete the CloudFormation stack.

- A. The configured timeout to delete the stack was too low for the delete operation to complete.
- B. The stack contains nested stacks that must be manually deleted first.
- C. The stack was deployed with the -disable rollback option.
- D. There are additional resources associated with a security group in the stack.
- E. There are Amazon S3 buckets that still contain objects in the stack.

Answer: DE

NEW QUESTION 140

- (Exam Topic 1)

A company is running a flash sale on its website. The website is hosted on burstable performance Amazon EC2 instances in an Auto Scaling group. The Auto Scaling group is configured to launch instances when the CPU utilization is above 70%.

A couple of hours into the sale, users report slow load times and error messages for refused connections. A SysOps administrator reviews Amazon CloudWatch metrics and notices that the CPU utilization is at 20% across the entire fleet of instances.

The SysOps administrator must restore the website's functionality without making changes to the network infrastructure.

Which solution will meet these requirements?

- A. Activate unlimited mode for the instances in the Auto Scaling group.
- B. Implement an Amazon CloudFront distribution to offload the traffic from the Auto Scaling group.
- C. Move the website to a different AWS Region that is closer to the users.
- D. Reduce the desired size of the Auto Scaling group to artificially increase CPU average utilization.

Answer: B

Explanation:

Implement an Amazon CloudFront distribution to offload the traffic from the Auto Scaling group does not breach the requirement of no changes in the network infrastructure. Reason is that cloudfront is a distribution that allows you to distribute content using a worldwide network of edge locations that provide low latency and high data transfer speeds. It plug in to existing setup, not changes to it.

NEW QUESTION 142

- (Exam Topic 1)

A company plans to deploy a database on an Amazon Aurora MySQL DB cluster. The database will store data for a demonstration environment. The data must be reset on a daily basis.

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

- A. Create a manual snapshot of the DB cluster after the data has been populate
- B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function on a daily basi
- C. Configure the function to restore the snapshot and then delete the previous DB cluster.
- D. Enable the Backtrack feature during the creation of the DB cluste
- E. Specify a target backtrack window of 48 hour
- F. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function on a daily basi
- G. Configure the function to perform a backtrack operation.
- H. Export a manual snapshot of the DB cluster to an Amazon S3 bucket after the data has been populated.Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function on a daily basi
- I. Configure the function to restore the snapshot from Amazon S3.
- J. Set the DB cluster backup retention period to 2 day
- K. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function on a daily basi
- L. Configure the function to restore the DB cluster to a point in time and then delete the previous DB cluster.

Answer: D

Explanation:

Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function on a daily basis. Configure the function to restore the DB cluster to a point in time and then delete the previous DB cluster. This is the most operationally efficient solution that meets the requirements, as it will allow the company to reset the database on a daily basis without having to manually take and restore snapshots. The other solutions (creating a manual snapshot of the DB cluster, enabling the Backtrack feature, or exporting a manual snapshot of the DB cluster to Amazon S3) will require additional steps and resources to reset the database on a daily basis.

NEW QUESTION 145

- (Exam Topic 1)

A company is using an Amazon DynamoDB table for data. A SysOps administrator must configure replication of the table to another AWS Region for disaster recovery.

What should the SysOps administrator do to meet this requirement?

- A. Enable DynamoDB Accelerator (DAX).
- B. Enable DynamoDB Streams, and add a global secondary index (GSI).
- C. Enable DynamoDB Streams, and-add a global table Region.
- D. Enable point-in-time recovery.

Answer: C

NEW QUESTION 149

- (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 152

- (Exam Topic 1)

A company's IT department noticed an increase in the spend of their developer AWS account. There are over 50 developers using the account, and the finance team wants to determine the service costs incurred by each developer.

What should a SysOps administrator do to collect this information? (Select TWO.)

- A. Activate the createdBy tag in the account.
- B. Analyze the usage with Amazon CloudWatch dashboards.
- C. Analyze the usage with Cost Explorer.
- D. Configure AWS Trusted Advisor to track resource usage.
- E. Create a billing alarm in AWS Budgets.

Answer: AC

NEW QUESTION 156

- (Exam Topic 1)

An application runs on multiple Amazon EC2 instances in an Auto Scaling group The Auto Scaling group is

configured to use the latest version of a launch template A SysOps administrator must devise a solution that centrally manages the application logs and retains the logs for no more than 90 days

Which solution will meet these requirements?

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

Answer: C

NEW QUESTION 160

- (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 163

- (Exam Topic 1)

A company has launched a social media website that gives users the ability to upload images directly to a centralized Amazon S3 bucket. The website is popular in areas that are geographically distant from the AWS Region where the S3 bucket is located. Users are reporting that uploads are slow. A SysOps administrator must improve the upload speed.

What should the SysOps administrator do to meet these requirements?

- A. Create S3 access points in Regions that are closer to the users.
- B. Create an accelerator in AWS Global Accelerator for the S3 bucket.
- C. Enable S3 Transfer Acceleration on the S3 bucket.
- D. Enable cross-origin resource sharing (CORS) on the S3 bucket.

Answer: C

Explanation:

You might want to use Transfer Acceleration on a bucket for various reasons: ->Your customers upload to a centralized bucket from all over the world. ->You transfer gigabytes to terabytes of data on a regular basis across continents. ->You can't use all of your available bandwidth over the internet when uploading to Amazon S3." <https://docs.aws.amazon.com/AmazonS3/latest/userguide/transfer-acceleration.html>

NEW QUESTION 164

- (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 bloque
- 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 bloque
- D. Use an origin access identity (OAI) to deliver the content through CloudFron

- 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 168

- (Exam Topic 1)

A company uses Amazon Route 53 to manage the public DNS records for the domain example.com. The company deploys an Amazon CloudFront distribution to deliver static assets for a new corporate website. The company wants to create a subdomain that is named "static" and must route traffic for the subdomain to the CloudFront distribution.

How should a SysOps administrator create a new record for the subdomain in Route 53?

- A. Create a CNAME record.
- B. Enter static.cloudfront.net as the record name.
- C. Enter the CloudFront distribution's public IP address as the value.
- D. Create a CNAME record.
- E. Enter static.example.com as the record name.
- F. Enter the CloudFront distribution's private IP address as the value.
- G. Create an A record.
- H. Enter static.cloudfront.net as the record name.
- I. Enter the CloudFront distribution's ID as an alias target.
- J. Create an A record.
- K. Enter static.example.com as the record name.
- L. Enter the CloudFront distribution's domain name as an alias target.

Answer: D

Explanation:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-cloudfront-distribution.html>

NEW QUESTION 173

- (Exam Topic 1)

A company plans to launch a static website on its domain example.com and subdomain www.example.com using Amazon S3. How should the SysOps administrator meet this requirement?

- A. Create one S3 bucket named example.com for both the domain and subdomain.
- B. Create one S3 bucket with a wildcard named *.example.com for both the domain and subdomain.
- C. Create two S3 buckets named example.com and www.example.com.
- D. Configure the subdomain bucket to redirect requests to the domain bucket.
- E. Create two S3 buckets named http://example.com and http://www.example.com.
- F. Configure the wildcard (*) bucket to redirect requests to the domain bucket.

Answer: C

NEW QUESTION 175

- (Exam Topic 1)

A company runs its Infrastructure on Amazon EC2 Instances that run in an Auto Scaling group. Recently, the company promoted faulty code to the entire EC2 fleet. This faulty code caused the Auto Scaling group to scale the instances before any of the application logs could be retrieved.

What should a SysOps administrator do to retain the application logs after instances are terminated?

- A. Configure an Auto Scaling lifecycle hook to create a snapshot of the ephemeral storage upon termination of the instances.
- B. Create a new Amazon Machine Image (AMI) that has the Amazon CloudWatch agent installed and configured to send logs to Amazon CloudWatch Log.
- C. Update the launch template to use the new AMI.
- D. Create a new Amazon Machine Image (AMI) that has a custom script configured to send logs to AWS CloudTrail.
- E. Update the launch template to use the new AMI.
- F. Install the Amazon CloudWatch agent on the Amazon Machine Image (AMI) that is defined in the launch template.
- G. Configure the CloudWatch agent to back up the logs to ephemeral storage.

Answer: B

NEW QUESTION 179

- (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 181

- (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 185

- (Exam Topic 1)

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

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

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

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

Answer: A

NEW QUESTION 190

- (Exam Topic 1)

A company wants to archive sensitive data on Amazon S3 Glacier. The company's regulatory and compliance requirements do not allow any modifications to the data by any account.

Which solution meets these requirements?

- A. Attach a vault lock policy to an S3 Glacier vault that contains the archived data
- B. Use the lock ID to validate the vault lock policy after 24 hours.
- C. Attach a vault lock policy to an S3 Glacier vault that contains the archived data
- D. Use the lock ID to validate the vault lock policy within 24 hours.
- E. Configure S3 Object Lock in governance mode
- F. Upload all files after 24 hours.
- G. Configure S3 Object Lock in governance mode
- H. Upload all files within 24 hours.

Answer: B

NEW QUESTION 192

- (Exam Topic 1)

A company's backend infrastructure contains an Amazon EC2 instance in a private subnet. The private subnet has a route to the internet through a NAT gateway in a public subnet. The instance must allow connectivity to a secure web server on the internet to retrieve data at regular intervals.

The client software times out with an error message that indicates that the client software could not establish the TCP connection.

What should a SysOps administrator do to resolve this error?

- A. Add an inbound rule to the security group for the EC2 instance with the following parameters: Type - HTTP, Source - 0.0.0.0/0.
- B. Add an inbound rule to the security group for the EC2 instance with the following parameters: Type - HTTPS, Source - 0.0.0.0/0.
- C. Add an outbound rule to the security group for the EC2 instance with the following parameters: Type - HTTP, Destination - 0.0.0.0/0.
- D. Add an outbound rule to the security group for the EC2 instance with the following parameters: Type - HTTP
- E. Destination - 0.0.0.0/0.

Answer: D

NEW QUESTION 193

- (Exam Topic 1)

A company is creating a new multi-account architecture. A Sysops administrator must implement a login solution to centrally manage user access and permissions across all AWS accounts. The solution must be integrated with AWS Organizations and must be connected to a third-party Security Assertion Markup Language (SAML) 2.0 identity provider (IdP).

What should the SysOps administrator do to meet these requirements?

- A. Configure an Amazon Cognito user pool
- B. Integrate the user pool with the third-party IdP.
- C. Enable and configure AWS Single Sign-On with the third-party IdP.
- D. Federate the third-party IdP with AWS Identity and Access Management (IAM) for each AWS account in the organization.
- E. Integrate the third-party IdP directly with AWS Organizations.

Answer: A

NEW QUESTION 198

- (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 tag
- 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-aws-lambda/>

NEW QUESTION 199

- (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 203

- (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 205

- (Exam Topic 1)

A company is using an AWS KMS customer master key (CMK) with imported key material. The company references the CMK by its alias in the Java application to encrypt data. The CMK must be rotated every 6 months. What is the process to rotate the key?

- A. Enable automatic key rotation for the CMK and specify a period of 6 months.
- B. Create a new CMK with new imported material, and update the key alias to point to the new CMK.
- C. Delete the current key material, and import new material into the existing CMK.
- D. Import a copy of the existing key material into a new CMK as a backup, and set the rotation schedule for 6 months.

Answer: B

NEW QUESTION 210

- (Exam Topic 1)

A SysOps administrator is investigating why a user has been unable to use RDP to connect over the internet from their home computer to a bastion server running on an Amazon EC2 Windows instance.

Which of the following are possible causes of this issue? (Choose two.)

- A. A network ACL associated with the bastion's subnet is blocking the network traffic.
- B. The instance does not have a private IP address.
- C. The route table associated with the bastion's subnet does not have a route to the internet gateway.
- D. The security group for the instance does not have an inbound rule on port 22.
- E. The security group for the instance does not have an outbound rule on port 3389.

Answer: AC

NEW QUESTION 213

- (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 218

- (Exam Topic 1)

A SysOps administrator needs to automate the invocation of an AWS Lambda function. The Lambda function must run at the end of each day to generate a report on data that is stored in an Amazon S3 bucket.

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

- A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that has an event pattern for Amazon S3 and the Lambda function as a target.
- B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that has a schedule and the Lambda function as a target.
- C. Create an S3 event notification to invoke the Lambda function whenever objects change in the S3 bucket.
- D. Deploy an Amazon EC2 instance with a cron job to invoke the Lambda function.

Answer: C

NEW QUESTION 221

- (Exam Topic 1)

A company has a simple web application that runs on a set of Amazon EC2 instances behind an Elastic Load Balancer in the eu-west-2 Region. Amazon Route 53 holds a DNS record for the application with a simple routing policy. Users from all over the world access the application through their web browsers.

The company needs to create additional copies of the application in the us-east-1 Region and in the ap-south-1 Region. The company must direct users to the Region that provides the fastest response times when the users load the application.

What should a SysOps administrator do to meet these requirements?

- A. In each new Region, create a new Elastic Load Balancer and a new set of EC2 instances to run a copy of the application.
- B. Transition to a geolocation routing policy.
- C. In each new Region, create a copy of the application on new EC2 instances.
- D. Add these new EC2 instances to the Elastic Load Balancer in eu-west-2. Transition to a latency routing policy.
- E. In each new Region, create a copy of the application on new EC2 instances.
- F. Add these new EC2 instances to the Elastic Load Balancer in eu-west-2. Transition to a multivalue routing policy.
- G. In each new Region, create a new Elastic Load Balancer and a new set of EC2 instances to run a copy of the application.
- H. Transition to a latency routing policy.

Answer: B

NEW QUESTION 223

- (Exam Topic 1)

A company has a stateless application that runs on four Amazon EC2 instances. The application requires four instances at all times to support all traffic. A SysOps administrator must design a highly available,

fault-tolerant architecture that continually supports all traffic if one Availability Zone becomes unavailable.

Which configuration meets these requirements?

- A. Deploy two Auto Scaling groups in two Availability Zones with a minimum capacity of two instances in each group.

- B. Deploy an Auto Scaling group across two Availability Zones with a minimum capacity of four instances.
- C. Deploy an Auto Scaling group across three Availability Zones with a minimum capacity of four instances.
- D. Deploy an Auto Scaling group across three Availability Zones with a minimum capacity of six instances.

Answer: C

NEW QUESTION 225

- (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 227

- (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 232

- (Exam Topic 1)

A company runs its entire suite of applications on Amazon EC2 instances. The company plans to move the applications to containers and AWS Fargate. Within 6 months, the company plans to retire its EC2 instances and use only Fargate. The company has been able to estimate its future Fargate costs.

A SysOps administrator needs to choose a purchasing option to help the company minimize costs. The SysOps administrator must maximize any discounts that are available and must ensure that there are no unused reservations.

Which purchasing option will meet these requirements?

- A. Compute Savings Plans for 1 year with the No Upfront payment option
- B. Compute Savings Plans for 1 year with the Partial Upfront payment option
- C. EC2 Instance Savings Plans for 1 year with the All Upfront payment option
- D. EC2 Reserved Instances for 1 year with the Partial Upfront payment option

Answer: C

NEW QUESTION 236

- (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 237

- (Exam Topic 1)

A web application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Auto Scaling group across multiple Availability Zones. A SysOps administrator notices that some of these EC2 instances show up as healthy in the Auto Scaling group but show up as unhealthy in the ALB target group.

What is a possible reason for this issue?

- A. Security groups are not allowing traffic between the ALB and the failing EC2 instances
- B. The Auto Scaling group health check is configured for EC2 status checks
- C. The EC2 instances are failing to launch and failing EC2 status checks.
- D. The target group health check is configured with an incorrect port or path

Answer: D

NEW QUESTION 240

- (Exam Topic 1)

A company runs a web application on three Amazon EC2 instances behind an Application Load Balancer (ALB). The company notices that random periods of increased traffic cause a degradation in the application's performance. A SysOps administrator must scale the application to meet the increased traffic. Which solution meets these requirements?

- A. Create an Amazon CloudWatch alarm to monitor application latency and increase the size of each EC2 instance if the desired threshold is reached.
- B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to monitor application latency and add an EC2 instance to the ALB if the desired threshold is reached.
- C. Deploy the application to an Auto Scaling group of EC2 instances with a target tracking scaling policy. Attach the ALB to the Auto Scaling group.
- D. Deploy the application to an Auto Scaling group of EC2 instances with a scheduled scaling policy. Attach the ALB to the Auto Scaling group.

Answer: C

NEW QUESTION 241

- (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 244

- (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 247

- (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 251

- (Exam Topic 1)

A company is running a website on Amazon EC2 instances that are in an Auto Scaling group. When the website traffic increases, additional instances take several minutes to become available because of a

long-running user data script that installs software. A SysOps administrator must decrease the time that is required (or new instances to become available

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

- A. Reduce the scaling thresholds so that instances are added before traffic increases
- B. Purchase Reserved Instances to cover 100% of the maximum capacity of the Auto Scaling group
- C. Update the Auto Scaling group to launch instances that have a storage optimized instance type
- D. Use EC2 Image Builder to prepare an Amazon Machine Image (AMI) that has pre-installed software

Answer: D

Explanation:

automated way to update your image. Have a pipeline to update your image. When you boot from your AMI updates = scripts are already pre-installed, so no need to complete boot scripts in boot process. <https://aws.amazon.com/image-builder/>

NEW QUESTION 256

- (Exam Topic 1)

A SysOps administrator is trying to set up an Amazon Route 53 domain name to route traffic to a website hosted on Amazon S3. The domain name of the website is `www.anycompany.com` and the S3 bucket name is `anycompany-static`. After the record set is set up in Route 53, the domain name `www.anycompany.com` does not seem to work, and the static website is not displayed in the browser.

Which of the following is a cause of this?

- A. The S3 bucket must be configured with Amazon CloudFront first.
- B. The Route 53 record set must have an IAM role that allows access to the S3 bucket.
- C. The Route 53 record set must be in the same region as the S3 bucket.
- D. The S3 bucket name must match the record set name in Route 53.

Answer: D

NEW QUESTION 258

- (Exam Topic 1)

A SysOps administrator has launched a large general purpose Amazon EC2 instance to regularly process large data files. The instance has an attached 1 TB General Purpose SSD (gp2) Amazon Elastic Block Store (Amazon EBS) volume. The instance also is EBS-optimized. To save costs, the SysOps administrator stops the instance each evening and restarts the instance each morning.

When data processing is active, Amazon CloudWatch metrics on the instance show a consistent 3,000 VolumeReadOps. The SysOps administrator must improve the I/O performance while ensuring data integrity.

Which action will meet these requirements?

- A. Change the instance type to a large, burstable, general purpose instance.
- B. Change the instance type to an extra large general purpose instance.
- C. Increase the EBS volume to a 2 TB General Purpose SSD (gp2) volume.
- D. Move the data that resides on the EBS volume to the instance store.

Answer: C

NEW QUESTION 262

- (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 266

- (Exam Topic 1)

A SysOps administrator needs to track the costs of data transfer between AWS Regions. The SysOps administrator must implement a solution to send alerts to an

email distribution list when transfer costs reach 75% of a specific threshold.
What should the SysOps administrator do to meet these requirements?

- A. Create an AWS Cost and Usage Repor
- B. Analyze the results in Amazon Athen
- C. Configure an alarm to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic when costs reach 75% of the threshol
- D. Subscribe the email distribution list to the topic.
- E. Create an Amazon CloudWatch billing alarm to detect when costs reach 75% of the threshold. Configure the alarm to publish a message to an Amazon Simple Notification Service (Amazon SNS) topi
- F. Subscribe the email distribution list to the topic.
- G. Use AWS Budgets to create a cost budget for data transfer cost
- H. Set an alert at 75% of the budgeted amoun
- I. Configure the budget to send a notification to the email distribution list when costs reach 75% of the threshold.
- J. Set up a VPC flow lo
- K. Set up a subscription filter to an AWS Lambda function to analyze data transfer. Configure the Lambda function to send a notification to the email distribution list when costs reach 75% of the threshold.

Answer: B

Explanation:

The reason is that it uses the Amazon CloudWatch billing alarm which is a built-in service specifically designed to monitor and alert on cost usage of your AWS account, which makes it a more suitable solution for this use case. The alarm can be configured to detect when costs reach 75% of the threshold and when it is triggered, it can publish a message to an Amazon Simple Notification Service (Amazon SNS) topic. The email distribution list can be subscribed to the topic, so that they will receive the alerts when costs reach 75% of the threshold.

AWS Budgets allows you to track and manage your costs, but it doesn't specifically focus on data transfer costs between regions, and it might not provide as much granularity as CloudWatch Alarms.

NEW QUESTION 271

- (Exam Topic 1)

A company's SysOps administrator deploys four new Amazon EC2 instances by using the standard Amazon Linux 2 Amazon Machine Image (AMI). The company needs to be able to use AWS Systems Manager to manage the instances The SysOps administrator notices that the instances do not appear in the Systems Manager console

What must the SysOps administrator do to resolve this issue?

- A. Connect to each instance by using SSH Install Systems Manager Agent on each instance Configure Systems Manager Agent to start automatically when the instances start up
- B. Use AWS Certificate Manager (ACM) to create a TLS certificate Import the certificate into each instance Configure Systems Manager Agent to use the TLS certificate for secure communications
- C. Connect to each instance by using SSH Create an ssm-user account Add the ssm-user account to the/etc/sudoers.d directory
- D. Attach an IAM instance profile to the instances Ensure that the instance profile contains the AmazonSSMManagedInstanceCore policy

Answer: D

NEW QUESTION 276

- (Exam Topic 1)

A company has a high-performance Windows workload. The workload requires a storage volume that provides consistent performance of 10,000 KDPS. The company does not want to pay for additional unneeded capacity to achieve this performance.

Which solution will meet these requirements with the LEAST cost?

- A. Use a Provisioned IOPS SSD (io1) Amazon Elastic Block Store (Amazon EBS) volume that is configured with 10,000 provisioned IOPS
- B. Use a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume that is configured with 10,000 provisioned IOPS.
- C. Use an Amazon Elastic File System (Amazon EFS) file system w\ Max I/O mode.
- D. Use an Amazon FSx for Windows File Server file system that is configured with 10,000 IOPS

Answer: A

NEW QUESTION 277

- (Exam Topic 1)

A company is expanding globally and needs to back up data on Amazon Elastic Block Store (Amazon EBS) volumes to a different AWS Region. Most of the EBS volumes that store the data are encrypted, but some of the EBS volumes are unencrypted. The company needs the backup data from all the EBS volumes to be encrypted.

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

- A. Configure a lifecycle policy in Amazon Data Lifecycle Manager (Amazon DLM) to create the EBS volume snapshots with cross-Region backups enable
- B. Encrypt the snapshot copies by using AWS Key Management Service (AWS KMS).
- C. Create a point-in-time snapshot of the EBS volume
- D. When the snapshot status is COMPLETED, copy the snapshots to another Region and set the Encrypted parameter to False.
- E. Create a point-in-time snapshot of the EBS volume
- F. Copy the snapshots to an Amazon S3 bucket that uses server-side encryption
- G. Turn on S3 Cross-Region Replication on the S3 bucket.
- H. Schedule an AWS Lambda function with the Python runtime
- I. Configure the Lambda function to create the EBS volume snapshots, encrypt the unencrypted snapshots, and copy the snapshots to another Region.

Answer: A

Explanation:

Encrypt the snapshot copies by using AWS Key Management Service (AWS KMS). This solution will allow the company to automatically create encrypted snapshots of the EBS volumes and copy them to different AWS Regions with minimal effort.

NEW QUESTION 282

- (Exam Topic 1)

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

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

Which action will meet these requirements?

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

Answer: A

Explanation:

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

NEW QUESTION 285

- (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 "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

NEW QUESTION 286

- (Exam Topic 1)

A company must migrate its applications to AWS The company is using Chef recipes for configuration management The company wants to continue to use the existing Chef recipes after the applications are migrated to AWS.

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

- A. Use AWS Cloud Format ion to create an Amazon EC2 instance, install a Chef server, and add Chefrecipes.
- B. Use AWS CloudFormation to create a stack and add layers for Chef recipes.
- C. Use AWS Elastic Beanstalk with the Docker platform to upload Chef recipes.
- D. Use AWS OpsWorks to create a stack and add layers with Chef recipes.

Answer: D

NEW QUESTION 290

- (Exam Topic 1)

A SysOps administrator is evaluating Amazon Route 53 DNS options to address concerns about high availability for an on-premises website. The website consists of two servers: a primary active server and a secondary passive server. Route 53 should route traffic to the primary server if the associated health check returns 2xx or 3xx HTTP codes. All other traffic should be directed to the secondary passive server. The failover record type, set ID. and routing policy have been set appropriately for both primary and secondary servers.

Which next step should be taken to configure Route 53?

- A. Create an A record for each serve
- B. Associate the records with the Route 53 HTTP health check.
- C. Create an A record for each serve
- D. Associate the records with the Route 53 TCP health check.
- E. Create an alias record for each server with evaluate target health set to ye
- F. Associate the records withthe Route 53 HTTP health check.
- G. Create an alias record for each server with evaluate target health set to ye
- H. Associate the records with the Route 53 TCP health check.

Answer: A

NEW QUESTION 292

- (Exam Topic 1)

An Amazon EC2 instance needs to be reachable from the internet. The EC2 instance is in a subnet with the following route table:

Destination	Target
10.0.0.0/16	Local
172.31.0.0/16	pcx-1122334455

Which entry must a SysOps administrator add to the route table to meet this requirement?

- A. A route for 0.0.0.0/0 that points to a NAT gateway
- B. A route for 0.0.0.0/0 that points to an egress-only internet gateway
- C. A route for 0.0.0.0/0 that points to an internet gateway
- D. A route for 0.0.0.0/0 that points to an elastic network interface

Answer: C

NEW QUESTION 296

- (Exam Topic 1)

A SysOps administrator has an AWS CloudFormation template of the company's existing infrastructure in us-west-2. The administrator attempts to use the template to launch a new stack in eu-west-1, but the stack only partially deploys, receives an error message, and then rolls back.

Why would this template fail to deploy? (Select TWO.)

- A. The template referenced an IAM user that is not available in eu-west-1.
- B. The template referenced an Amazon Machine Image (AMI) that is not available in eu-west-1.
- C. The template did not have the proper level of permissions to deploy the resources.
- D. The template requested services that do not exist in eu-west-1.
- E. CloudFormation templates can be used only to update existing services.

Answer: BD

NEW QUESTION 300

- (Exam Topic 1)

A company needs to ensure strict adherence to a budget for 25 applications deployed on AWS. Separate teams are responsible for storage, compute, and database costs. A SysOps administrator must implement an automated solution to alert each team when their projected spend will exceed a quarterly amount that has been set by the finance department. The solution cannot add additional compute, storage, or database costs.

- A. Configure AWS Cost and Usage Reports to send a daily report to an Amazon S3 bucket
- B. Create an AWS Lambda function that will evaluate spend by service and notify each team by using Amazon Simple Notification Service (Amazon SNS) notification
- C. Invoke the Lambda function when a report is placed in the S3 bucket
- D. Configure AWS Cost and Usage Reports to send a daily report to an Amazon S3 bucket
- E. Create a rule in Amazon EventBridge (Amazon CloudWatch Events) to evaluate the spend by service and notify each team by using Amazon Simple Queue Service (Amazon SQS) when the cost threshold is exceeded.
- F. Use AWS Budgets to create one cost budget and select each of the services in use. Specify the budget amount defined by the finance department along with the forecasted cost threshold. Enter the appropriate email recipients for the budget.
- G. Use AWS Budgets to create a cost budget for each team, filtering by the services they own
- H. Specify the budget amount defined by the finance department along with a forecasted cost threshold. Enter the appropriate email recipients for each budget.

Answer: D

NEW QUESTION 302

- (Exam Topic 1)

A company is expanding its use of AWS services across its portfolios. The company wants to provision AWS accounts for each team to ensure a separation of business processes for security compliance and billing. Account creation and bootstrapping should be completed in a scalable and efficient way so new accounts are created with a defined baseline and governance guardrails in place. A SysOps administrator needs to design a provisioning process that saves time and resources.

Which action should be taken to meet these requirements?

- A. Automate using AWS Elastic Beanstalk to provision the AWS accounts, set up infrastructure, and integrate with AWS Organizations
- B. Create bootstrapping scripts in AWS OpsWorks and combine them with AWS CloudFormation templates to provision accounts and infrastructure
- C. Use AWS Config to provision accounts and deploy instances using AWS Service Catalog
- D. Use AWS Control Tower to create a template in Account Factory and use the template to provision new accounts

Answer: D

NEW QUESTION 306

- (Exam Topic 1)

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

Which solution will meet these requirements MOST cost-effectively?

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

- F. Set up an S3 Lifecycle rule to move the data to S3 Glacier Flexible Retrieval after 90 days.
- G. Store the data in S3 Standard for the first 90 day
- H. Set up an S3 Lifecycle rule to move the data to S3 Glacier Deep Archive after 90 days.

Answer: A

Explanation:

Glacier Deep Archive retrieval time more than 5 hours (it's 12 hours), so B&D out. S3 Standard IA is cheaper than S3 Standard.
<https://aws.amazon.com/tw/s3/pricing/>

NEW QUESTION 311

- (Exam Topic 1)

A compliance team requires all administrator passwords for Amazon RDS DB instances to be changed at least annually. Which solution meets this requirement in the MOST operationally efficient manner?

- A. Store the database credentials in AWS Secrets Manager. Configure automatic rotation for the secret every 365 days.
- B. Store the database credentials as a parameter in the RDS parameter group. Create a database trigger to rotate the password every 365 days.
- C. Store the database credentials in a private Amazon S3 bucket. Schedule an AWS Lambda function to generate a new set of credentials every 365 days.
- D. Store the database credentials in AWS Systems Manager Parameter Store as a secure string parameter. Configure automatic rotation for the parameter every 365 days.

Answer: A

NEW QUESTION 313

- (Exam Topic 1)

A data storage company provides a service that gives users the ability to upload and download files as needed. The files are stored in Amazon S3 Standard and must be immediately retrievable for 1 year. Users access files frequently during the first 30 days after the files are stored. Users rarely access files after 30 days. The company's SysOps administrator must use S3 Lifecycle policies to implement a solution that maintains object availability and minimizes cost. Which solution will meet these requirements?

- A. Move objects to S3 Glacier after 30 days.
- B. Move objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.
- C. Move objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
- D. Move objects to S3 Standard-Infrequent Access (S3 Standard-IA) immediately.

Answer: C

Explanation:

<https://aws.amazon.com/s3/storage-classes/>

NEW QUESTION 317

- (Exam Topic 1)

A company monitors its account activity using AWS CloudTrail and is concerned that some log files are being tampered with after the logs have been delivered to the account's Amazon S3 bucket. Moving forward, how can the SysOps administrator confirm that the log files have not been modified after being delivered to the S3 bucket?

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

Answer: B

Explanation:

When you enable log file integrity validation, CloudTrail creates a hash for every log file that it delivers. Every hour, CloudTrail also creates and delivers a file that references the log files for the last hour and contains a hash of each. This file is called a digest file. CloudTrail signs each digest file using the private key of a public and private key pair. After delivery, you can use the public key to validate the digest file. CloudTrail uses different key pairs for each AWS region.
<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html>

NEW QUESTION 322

- (Exam Topic 1)

A recent organizational audit uncovered an existing Amazon RDS database that is not currently configured for high availability. Given the critical nature of this database, it must be configured for high availability as soon as possible. How can this requirement be met?

- A. Switch to an active/passive database pair using the create-db-instance-read-replica with the --availability-zone flag.
- B. Specify high availability when creating a new RDS instance, and live-migrate the data.
- C. Modify the RDS instance using the console to include the Multi-AZ option.
- D. Use the modify-db-instance command with the --na flag.

Answer: C

NEW QUESTION 325

- (Exam Topic 1)

A team of On-call engineers frequently needs to connect to Amazon EC2 instances in a private subnet to troubleshoot and run commands. The instances use either the latest AWS-provided Windows Amazon Machine Images (AMIs) or Amazon Linux AMIs. The team has an existing IAM role for authorization. A SysOps administrator must provide the team with access to the instances by granting IAM permissions to this. Which solution will meet this requirement?

- A. Add a statement to the IAM role policy to allow the ssm:StartSession action on the instance
- B. Instruct the team to use AWS Systems Manager Session Manager to connect to the Instances by using the assumed IAM role.
- C. Associate an Elastic IP address and a security group with each instance
- D. Add the engineers' IP addresses to the security group inbound rule
- E. Add a statement to the IAM role policy to allow the ec2:AuthorizeSecurityGroupIngress action so that the team can connect to the Instances.
- F. Create a bastion host with an EC2 Instance, and associate the bastion host with the VP
- G. Add a statement to the IAM role policy to allow the ec2:CreateVpnConnection action on the bastion host
- H. Instruct the team to use the bastion host endpoint to connect to the instances.
- I. Use two listeners
- J. Forward port 22 to a target group of Linux instance
- K. Forward port 3389 to a target group of Windows Instance
- L. Add a statement to the IAM role policy to allow the ec2:CreateRoute action so that the team can connect to the Instances.

Answer: A

NEW QUESTION 327

- (Exam Topic 1)

With the threat of ransomware viruses encrypting and holding company data hostage, which action should be taken to protect an Amazon S3 bucket?

- A. Deny Pos
- B. Put
- C. and Delete on the bucket.
- D. Enable server-side encryption on the bucket.
- E. Enable Amazon S3 versioning on the bucket.
- F. Enable snapshots on the bucket.

Answer: B

NEW QUESTION 329

- (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 331

- (Exam Topic 1)

A company uses an Amazon Elastic File System (Amazon EFS) file system to share files across many Linux Amazon EC2 instances. A SysOps administrator notices that the file system's PercentIOLimit metric is consistently at 100% for 15 minutes or longer. The SysOps administrator also notices that the application that reads and writes to that file system is performing poorly. The application requires high throughput and IOPS while accessing the file system. What should the SysOps administrator do to remediate the consistently high PercentIOLimit metric?

- A. Create a new EFS file system that uses Max I/O performance mode.
- B. Use AWS DataSync to migrate data to the new EFS file system.
- C. Create an EFS lifecycle policy to transition future files to the Infrequent Access (IA) storage class to improve performance.
- D. Use AWS DataSync to migrate existing data to IA storage.
- E. Modify the existing EFS file system and activate Max I/O performance mode.
- F. Modify the existing EFS file system and activate Provisioned Throughput mode.

Answer: A

Explanation:

To support a wide variety of cloud storage workloads, Amazon EFS offers two performance modes, General Purpose mode and Max I/O mode. You choose a file system's performance mode when you create it, and it cannot be changed. If the PercentIOLimit percentage returned was at or near 100 percent for a significant amount of time during the test, your application should use the Max I/O performance mode. <https://docs.aws.amazon.com/efs/latest/ug/performance.html>

NEW QUESTION 332

- (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 exarrc4e.com to the on-premises DNS servers Associate this rule with the VPC.

Answer: C

NEW QUESTION 334

- (Exam Topic 1)

A SysOps administrator is reviewing VPC Flow Logs to troubleshoot connectivity issues in a VPC. While reviewing the logs the SysOps administrator notices that rejected traffic is not listed.

What should the SysOps administrator do to ensure that all traffic is logged?

- A. Create a new flow log that has a filter setting to capture all traffic
- B. Create a new flow log set the log record format to a custom format Select the proper fields to include in the log
- C. Edit the existing flow log Change the filter setting to capture all traffic
- D. Edit the existing flow log
- E. Set the log record format to a custom format Select the proper fields to include in the log

Answer: A

NEW QUESTION 339

- (Exam Topic 1)

An AWS Lambda function is intermittently failing several times a day A SysOps administrator must find out how often this error has occurred in the last 7 days

Which action will meet this requirement in the MOST operationally efficient manner?

- A. Use Amazon Athena to query the Amazon CloudWatch logs that are associated with the Lambda function
- B. Use Amazon Athena to query the AWS CloudTrail logs that are associated with the Lambda function
- C. Use Amazon CloudWatch Logs Insights to query the associated Lambda function logs
- D. Use Amazon Elasticsearch Service (Amazon ES) to stream the Amazon CloudWatch logs for the Lambda function

Answer: C

NEW QUESTION 343

- (Exam Topic 1)

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

What should a SysOps administrator do to resolve these errors?

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

Answer: B

Explanation:

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

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

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

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

NEW QUESTION 345

- (Exam Topic 1)

A manufacturing company uses an Amazon RDS DB instance to store inventory of all stock items. The company maintains several AWS Lambda functions that interact with the database to add, update, and delete items. The Lambda functions use hardcoded credentials to connect to the database.

A SysOps administrator must ensure that the database credentials are never stored in plaintext and that the password is rotated every 30 days.

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

- A. Store the database password as an environment variable for each Lambda function
- B. Create a new Lambda function that is named PasswordRotate
- C. Use Amazon EventBridge (Amazon CloudWatch Events) to schedule the PasswordRotate function every 30 days to change the database password and update the environment variable for each Lambda function.
- D. Use AWS Key Management Service (AWS KMS) to encrypt the database password and to store the encrypted password as an environment variable for each Lambda function
- E. Grant each Lambda function access to the KMS key so that the database password can be decrypted when required
- F. Create a new Lambda function that is named PasswordRotate to change the password every 30 days.
- G. Use AWS Secrets Manager to store credentials for the database
- H. Create a Secrets Manager secret, and select the database so that Secrets Manager will use a Lambda function to update the database password automatically
- I. Specify an automatic rotation schedule of 30 days
- J. Update each Lambda function to access the database password from Secrets Manager.
- K. Use AWS Systems Manager Parameter Store to create a secure string to store credentials for the database
- L. Create a new Lambda function called PasswordRotate
- M. Use Amazon EventBridge (Amazon CloudWatch Events) to schedule the PasswordRotate function every 30 days to change the database password and to update the secret within Parameter Store
- N. Update each Lambda function to access the database password from Parameter Store.

Answer: C

Explanation:

When you choose to enable rotation, Secrets Manager supports the following Amazon Relational Database Service (Amazon RDS) databases with AWS written and tested Lambda rotation function templates, and full configuration of the rotation process:

Amazon Aurora on Amazon RDS MySQL on Amazon RDS PostgreSQL on Amazon RDS Oracle on Amazon RDS MariaDB on Amazon RDS

Microsoft SQL Server on Amazon RDS <https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html>

NEW QUESTION 349

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual AWS-SysOps Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the AWS-SysOps Product From:

<https://www.2passeasy.com/dumps/AWS-SysOps/>

Money Back Guarantee

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