

Exam Questions SOA-C02

AWS Certified SysOps Administrator - Associate (SOA-C02)

<https://www.2passeasy.com/dumps/SOA-C02/>



NEW QUESTION 1

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

Answer: A

NEW QUESTION 2

- (Exam Topic 1)

A company creates a new member account by using AWS Organizations. A SysOps administrator needs to add AWS Business Support to the new account

Which combination of steps must the SysOps administrator take to meet this requirement? (Select TWO.)

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

Answer: BE

Explanation:

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

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

Reference:

[1] https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_access.html#orgs_ma

NEW QUESTION 3

- (Exam Topic 1)

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

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

What is the result of this policy?

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

Answer: B

NEW QUESTION 4

- (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 5

- (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 6

- (Exam Topic 1)

The security team is concerned because the number of AWS Identity and Access Management (IAM) policies being used in the environment is increasing. The team tasked a SysOps administrator to report on the current number of IAM policies in use and the total available IAM policies.

Which AWS service should the administrator use to check how current IAM policy usage compares to current service limits?

- A. AWS Trusted Advisor
- B. Amazon Inspector
- C. AWS Config
- D. AWS Organizations

Answer: A

NEW QUESTION 7

- (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 8

- (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 E

- 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 E
- 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 domai
- 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 VP
- H. Create a security group that allows inbound traffic from the branch office CIDR blocks.

Answer: B

NEW QUESTION 9

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

Answer: C

NEW QUESTION 10

- (Exam Topic 1)

A company has deployed AWS Security Hub and AWS Config in a newly implemented organization in AWS Organizations. A SysOps administrator must implement a solution to restrict all member accounts in the organization from deploying Amazon EC2 resources in the ap-southeast-2 Region. The solution must be implemented from a single point and must govern an current and future accounts. The use of root credentials also must be restricted in member accounts. Which AWS feature should the SysOps administrator use to meet these requirements?

- A. AWS Config aggregator
- B. IAM user permissions boundaries
- C. AWS Organizations service control policies (SCPs)
- D. AWS Security Hub conformance packs

Answer: C

NEW QUESTION 10

- (Exam Topic 1)

A SysOps administrator recently configured Amazon S3 Cross-Region Replication on an S3 bucket Which of the following does this feature replicate to the destination S3 bucket by default?

- A. Objects in the source S3 bucket for which the bucket owner does not have permissions
- B. Objects that are stored in S3 Glacier
- C. Objects that existed before replication was configured
- D. Object metadata

Answer: B

NEW QUESTION 15

- (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 20

- (Exam Topic 1)

A SysOps administrator is reviewing AWS Trusted Advisor recommendations. The SysOps administrator notices that all the application servers for a finance application are listed in the Low Utilization Amazon EC2 Instances check. The application runs on three instances across three Availability Zones. The SysOps administrator must reduce the cost of running the application without affecting the application's availability or design.

Which solution will meet these requirements?

- A. Reduce the number of application servers.
- B. Apply rightsizing recommendations from AWS Cost Explorer to reduce the instance size.
- C. Provision an Application Load Balancer in front of the instances.
- D. Scale up the instance size of the application servers.

Answer: C

NEW QUESTION 22

- (Exam Topic 1)

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

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

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

Answer: AD

NEW QUESTION 26

- (Exam Topic 1)

A SysOps administrator needs to create alerts that are based on the read and write metrics of Amazon Elastic Block Store (Amazon EBS) volumes that are attached to an Amazon EC2 instance. The SysOps administrator creates and enables Amazon CloudWatch alarms for the DiskReadBytes metric and the DiskWriteBytes metric.

A custom monitoring tool that is installed on the EC2 instance with the same alarm configuration indicates that the volume metrics have exceeded the threshold.

However, the CloudWatch alarms were not in ALARM state.

Which action will ensure that the CloudWatch alarms function correctly?

- A. Install and configure the CloudWatch agent on the EC2 instance to capture the desired metrics.
- B. Install and configure AWS Systems Manager Agent on the EC2 instance to capture the desired metrics.
- C. Reconfigure the CloudWatch alarms to use the VolumeReadBytes metric and the VolumeWriteBytes metric for the EBS volumes.
- D. Reconfigure the CloudWatch alarms to use the VolumeReadBytes metric and the VolumeWriteBytes metric for the EC2 instance.

Answer: A

NEW QUESTION 30

- (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 32

- (Exam Topic 1)

A SysOps administrator must create an IAM policy for a developer who needs access to specific AWS services. Based on the requirements, the SysOps administrator creates the following policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "storagegateway:Describe*",
        "elasticloadbalancing:*",
        "lambda:*",
        "sqs:List*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Which actions does this policy allow? (Select TWO.)

- A. Create an AWS Storage Gateway.
- B. Create an IAM role for an AWS Lambda function.
- C. Delete an Amazon Simple Queue Service (Amazon SQS) queue.
- D. Describe AWS load balancers.
- E. Invoke an AWS Lambda function.

Answer: DE

NEW QUESTION 37

- (Exam Topic 1)

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

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

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

Answer: B

NEW QUESTION 39

- (Exam Topic 1)

A company wants to create an automated solution for all accounts managed by AWS Organizations to detect any worry groups that urn 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 corresponds with the company's intranet.

- A. Create an AWS Config rule to detect noncompliant security group
- B. Set up automatic remediation to change the 0.0.0.0/0 source address to the approved CIDK 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 1AM policy to every user in the company.
- D. Create an AWS Lambda function to inspect now and existing security groups check for a noncompliant 0.0.0.0A) 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 Vie 0.0.0.0/0 source address to the approved CIDR block.

Answer: A

NEW QUESTION 42

- (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 objec
- D. Save the tags in a lis
- E. Use S3 Batch Operations.Specify the operation to delete all object tag
- F. Use the AWS CLI and the list to retag the objects.
- G. Use the AWS CLI to get the tags for each objec
- H. Save the tags in a lis
- I. Use the AWS CLI and the list to remove the object tag
- J. Use the AWS CLI and the list to retag the objects.
- K. Use the AWS CLI to copy the objects to another S3 bucke
- 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 44

- (Exam Topic 1)

A company has an internal web application that runs on Amazon EC2 instances behind an Application Load

Balancer. The instances run in an Amazon EC2 Auto Scaling group in a single Availability Zone. A SysOps administrator must make the application highly available.

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

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

Answer: C

NEW QUESTION 45

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

Answer: A

Explanation:

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

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

NEW QUESTION 49

- (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

Explanation:

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

NEW QUESTION 54

- (Exam Topic 1)

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

Where can the administrator find this information?

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

Answer: D

Explanation:

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

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

NEW QUESTION 57

- (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 58

- (Exam Topic 1)

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

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

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

Answer: D

NEW QUESTION 60

- (Exam Topic 1)

A company uses an AWS CloudFormation template to provision an Amazon EC2 instance and an Amazon RDS DB instance A SysOps administrator must update the template to ensure that the DB instance is created before the EC2 instance is launched

What should the SysOps administrator do to meet this requirement?

- A. Add a wait condition to the template Update the EC2 instance user data script to send a signal after the EC2 instance is started
- B. Add the DependsOn attribute to the EC2 instance resource, and provide the logical name of the RDS resource
- C. Change the order of the resources in the template so that the RDS resource is listed before the EC2 instance resource
- D. Create multiple templates Use AWS CloudFormation StackSets to wait for one stack to complete before the second stack is created

Answer: B

Explanation:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-dependson.html> Syntax The DependsOn attribute can take a single string or list of strings. "DependsOn" : [String, ...]

Example The following template contains an `AWS::EC2::Instance` resource with a DependsOn attribute that specifies `myDB`, an `AWS::RDS::DBInstance`. When CloudFormation creates this stack, it first creates `myDB`, then creates `Ec2Instance`.

NEW QUESTION 62

- (Exam Topic 1)

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

Which action will allow the SysOps administrator to remotely connect to the instance?

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

Answer: C

NEW QUESTION 64

- (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 68

- (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 69

- (Exam Topic 1)

A SysOps administrator has successfully deployed a VPC with an AWS Cloud Formation template The SysOps administrator wants to deploy me same template across multiple accounts that are managed through AWS Organizations.

Which solution will meet this requirement with the LEAST operational overhead?

- A. Assume the OrganizationAccountAcccssKolc IAM role from the management accoun
- B. Deploy the template in each of the accounts
- C. Create an AWS Lambda function to assume a role in each account Deploy the template by using the AWS CloudFormation CreateStack API call
- D. Create an AWS Lambda function to query fc a list of accounts Deploy the template by using the AWS Cloudformation CreateStack API call.
- E. Use AWS CloudFormation StackSets from the management account to deploy the template in each of the accounts

Answer: D

Explanation:

AWS CloudFormation StackSets extends the capability of stacks by enabling you to create, update, or delete stacks across multiple accounts and AWS Regions

NEW QUESTION 74

- (Exam Topic 1)

A SysOps administrator is unable to launch Amazon EC2 instances into a VPC because there are no available private IPv4 addresses in the VPC. Which combination of actions must the SysOps administrator take to launch the instances? (Select TWO.)

- A. Associate a secondary IPv4 CIDR block with the VPC
- B. Associate a primary IPv6 CIDR block with the VPC
- C. Create a new subnet for the VPC
- D. Modify the CIDR block of the VPC
- E. Modify the CIDR block of the subnet that is associated with the instances

Answer: AD

NEW QUESTION 77

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

Answer: C

Explanation:

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

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Managing.Backtrack.html>

NEW QUESTION 81

- (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 83

- (Exam Topic 1)

A SysOps administrator Is troubleshooting an AWS Cloud Formation template whereby multiple Amazon EC2 instances are being created The template is working

In us-east-1. but it is failing In us-west-2 with the error code:

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

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

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

Answer: A

NEW QUESTION 88

- (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 91

- (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 95

- (Exam Topic 1)

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

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

Which action will resolve this issue?

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

Answer: C

NEW QUESTION 99

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

queue for email notification each time that usage exceeds 60% of one of the service quotas.

F. Use the AWS Service Health Dashboard to monitor each Trusted Advisor service quota metric. Configure an Amazon Simple Notification Service (Amazon SNS) topic for email notification each time that usage exceeds 60% of one of the service quotas.

Answer: A

Explanation:

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

NEW QUESTION 104

- (Exam Topic 1)

A company recently acquired another corporation and all of that corporation's AWS accounts. A financial analyst needs the cost data from these accounts. A SysOps administrator uses Cost Explorer to generate cost and usage reports. The SysOps administrator notices that "No Tagkey" represents 20% of the monthly cost.

What should the SysOps administrator do to tag the "No Tagkey" resources?

- A. Add the accounts to AWS Organization
- B. Use a service control policy (SCP) to tag all the untagged resources.
- C. Use an AWS Config rule to find the untagged resource
- D. Set the remediation action to terminate the resources.
- E. Use Cost Explorer to find and tag all the untagged resources.
- F. Use Tag Editor to find and tag all the untagged resources.

Answer: D

Explanation:

"You can add tags to resources when you create the resource. You can use the resource's service console or API to add, change, or remove those tags one resource at a time. To add tags to—or edit or delete tags of—multiple resources at once, use Tag Editor. With Tag Editor, you search for the resources that you want to tag, and then manage tags for the resources in your search results." <https://docs.aws.amazon.com/ARG/latest/userguide/tag-editor.html>

NEW QUESTION 105

- (Exam Topic 1)

A SysOps administrator must create a solution that automatically shuts down any Amazon EC2 instances that have less than 10% average CPU utilization for 60 minutes or more.

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

- A. Implement a cron job on each EC2 instance to run once every 60 minutes and calculate the current CPU utilization
- B. Initiate an instance shutdown if CPU utilization is less than 10%.
- C. Implement an Amazon CloudWatch alarm for each EC2 instance to monitor average CPU utilization. Set the period at 1 hour, and set the threshold at 10%. Configure an EC2 action on the alarm to stop the instance.
- D. Install the unified Amazon CloudWatch agent on each EC2 instance, and enable the Basic level predefined metric set
- E. Log CPU utilization every 60 minutes, and initiate an instance shutdown if CPU utilization is less than 10%.
- F. Use AWS Systems Manager Run Command to get CPU utilization from each EC2 instance every 60 minutes
- G. Initiate an instance shutdown if CPU utilization is less than 10%.

Answer: B

Explanation:

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

NEW QUESTION 106

- (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 111

- (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 116

- (Exam Topic 1)

A company uses AWS Organizations to manage multiple AWS accounts. The company's SysOps team has been using a manual process to create and manage 1AM roles. The team requires an automated solution to create and manage the necessary 1AM roles for multiple AWS accounts.

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

- A. Create AWS CloudFormation template
- B. Reuse the templates to create the necessary 1AM roles in each of the AWS accounts.
- C. Use AWS Directory Service with AWS Organizations to automatically associate the necessary 1AM roles with Microsoft Active Directory users.
- D. Use AWS Resource Access Manager with AWS Organizations to deploy and manage shared resources across the AWS accounts.
- E. Use AWS CloudFormation StackSets with AWS Organizations to deploy and manage 1AM roles for the AWS accounts.

Answer: D

NEW QUESTION 120

- (Exam Topic 1)

An organization is running multiple applications for their customers. Each application is deployed by running a base AWS CloudFormation template that configures a new VPC. All applications are run in the same AWS account and AWS Region. A SysOps administrator has noticed that when trying to deploy the same AWS CloudFormation stack, it fails to deploy. What is likely to be the problem?

- A. The Amazon Machine image used is not available in that region.
- B. The AWS CloudFormation template needs to be updated to the latest version.
- C. The VPC configuration parameters have changed and must be updated in the template.
- D. The account has reached the default limit for VPCs allowed.

Answer: D

NEW QUESTION 121

- (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 126

- (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
- B. Share the user credentials with the security administrator.
- C. Create an IAM policy in each developer account that has administrator access to all Amazon EC2 actions, including VPC action
- D. Assign the policy to an IAM user
- E. Share the user credentials with the security administrator.
- F. 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
- G. Ask the security administrator to assume the role from their account.
- H. 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 131

- (Exam Topic 1)

A SysOps administrator is responsible for a large fleet of Amazon EC2 instances and must know whether any instances will be affected by upcoming hardware maintenance. Which option would provide this information with the LEAST administrative overhead?

- A. Deploy a third-party monitoring solution to provide real-time EC2 instance monitoring

- B. List any instances with failed system status checks using the AWS Management Console
- C. Monitor AWS CloudTrail for Stopinstances API calls
- D. Review the AWS Personal Health Dashboard

Answer: D

Explanation:

<https://docs.aws.amazon.com/health/latest/ug/cloudwatch-events-health.html>

NEW QUESTION 133

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/redis-cluster-vertical-scaling-scaling-down.html>

NEW QUESTION 138

- (Exam Topic 1)

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

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 139

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

Answer: C

NEW QUESTION 142

- (Exam Topic 1)

A development team recently deployed a new version of a web application to production. After the release, penetration testing revealed a cross-site scripting vulnerability that could expose user data.

Which AWS service will mitigate this issue?

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

Answer: B

NEW QUESTION 146

- (Exam Topic 1)

A company has an application that customers use to search for records on a website. The application's data is stored in an Amazon Aurora DB cluster. The application's usage varies by season and by day of the week.

The website's popularity is increasing, and the website is experiencing slower performance because of increased load on the DB cluster during periods of peak activity. The application logs show that the performance issues occur when users are searching for information. The same search is rarely performed multiple times.

A SysOps administrator must improve the performance of the platform by using a solution that maximizes resource efficiency.

Which solution will meet these requirements?

- A. Deploy an Amazon ElastiCache for Redis cluster in front of the DB cluster
- B. Modify the application to check the cache before the application issues new queries to the database
- C. Add the results of any queries to the cache.
- D. Deploy an Aurora Replica for the DB cluster
- E. Modify the application to use the reader endpoint for search operation
- F. Use Aurora Auto Scaling to scale the number of replicas based on load
- G. Most Voted
- H. Use Provisioned IOPS on the storage volumes that support the DB cluster to improve performance sufficiently to support the peak load on the application.
- I. Increase the instance size in the DB cluster to a size that is sufficient to support the peak load on the application
- J. Use Aurora Auto Scaling to scale the instance size based on load.

Answer: B

Explanation:

https://docs.amazonaws.cn/en_us/AmazonRDS/latest/AuroraUserGuide/aurora-replicas-adding.html

NEW QUESTION 148

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

Answer: B

Explanation:

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

NEW QUESTION 151

- (Exam Topic 1)

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

How should a SysOps administrator remediate this issue?

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

Answer: A

NEW QUESTION 154

- (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 populated
- B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function on a daily basis
- 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 cluster
- E. Specify a target backtrack window of 48 hours
- F. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function on a daily basis
- 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 basis
- I. Configure the function to restore the snapshot from Amazon S3.
- J. Set the DB cluster backup retention period to 2 days
- K. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function on a daily basis

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 158

- (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 162

- (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 167

- (Exam Topic 1)

A company stores critical data in Amazon S3 buckets. A SysOps administrator must build a solution to record all S3 API activity. Which action will meet this requirement?

- A. Configure S3 bucket metrics to record object access logs
- B. Create an AWS CloudTrail trail to log data events for all S3 objects
- C. Enable S3 server access logging for each S3 bucket
- D. Use AWS IAM Access Analyzer for Amazon S3 to store object access logs.

Answer: B

NEW QUESTION 170

- (Exam Topic 1)

A company needs to deploy a new workload on AWS. The company must encrypt all data at rest and must rotate the encryption keys once each year. The workload uses an Amazon RDS for MySQL Multi-AZ database for data storage.

Which configuration approach will meet these requirements?

- A. Enable Transparent Data Encryption (TDE) in the MySQL configuration file
- B. Manually rotate the key every 12 months.
- C. Enable RDS encryption on the database at creation time by using the AWS managed key for Amazon RDS.
- D. Create a new AWS Key Management Service (AWS KMS) customer managed key
- E. Enable automatic key rotation
- F. Enable RDS encryption on the database at creation time by using the KMS key.
- G. Create a new AWS Key Management Service (AWS KMS) customer managed key
- H. Enable automatic key rotation
- I. Enable encryption on the Amazon Elastic Block Store (Amazon EBS) volumes that are attached to the RDS DB instance.

Answer: C

Explanation:

This configuration approach will meet the requirement of encrypting all data at rest and rotating the encryption keys once each year. By creating a new AWS KMS customer managed key and enabling automatic key rotation, the encryption keys will be rotated automatically every year. By enabling RDS encryption on the database at creation time using the KMS key, all data stored in the RDS for MySQL Multi-AZ database will be encrypted at rest. This approach provides more

control over key management and rotation and provide additional security benefits.

NEW QUESTION 172

- (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 177

- (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 EFS) 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 179

- (Exam Topic 1)

A company hosts a database on an Amazon RDS Multi-AZ DB instance. The database is not encrypted. The company's new security policy requires all AWS resources to be encrypted at rest and in transit. What should a SysOps administrator do to encrypt the database?

- A. Configure encryption on the existing DB instance.
- B. Take a snapshot of the DB instance.
- C. Encrypt the snapshot.
- D. Restore the snapshot to the same DB instance.
- E. Encrypt the standby replica in a secondary Availability Zone.
- F. Promote the standby replica to the primary DB instance.
- G. Take a snapshot of the DB instance.
- H. Copy and encrypt the snapshot.
- I. Create a new DB instance by restoring the encrypted copy.

Answer: B

NEW QUESTION 182

- (Exam Topic 1)

A company has a public website that recently experienced problems. Some links led to missing webpages, and other links rendered incorrect webpages. The application infrastructure was running properly, and all the provisioned resources were healthy. Application logs and dashboards did not show any errors, and no monitoring alarms were raised. Systems administrators were not aware of any problems until end users reported the issues. The company needs to proactively monitor the website for such issues in the future and must implement a solution as soon as possible. Which solution will meet these requirements with the LEAST operational overhead?

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

Answer: A

NEW QUESTION 183

- (Exam Topic 1)

A company's public website is hosted in an Amazon S3 bucket in the us-east-1 Region behind an Amazon CloudFront distribution. The company wants to ensure that the website is protected from DDoS attacks. A SysOps administrator needs to deploy a solution that gives the company the ability to maintain control over the rate limit at which DDoS protections are applied. Which solution will meet these requirements?

- A. Deploy a global-scoped AWS WAF web ACL with an allow default action
- B. Configure an AWS WAF rate-based rule to block matching traffic
- C. Associate the web ACL with the CloudFront distribution.
- D. Deploy an AWS WAF web ACL with an allow default action in us-east-1. Configure an AWS WAF rate-based rule to block matching traffic
- E. Associate the web ACL with the S3 bucket.
- F. Deploy a global-scoped AWS WAF web ACL with a block default action
- G. Configure an AWS WAF rate-based rule to allow matching traffic
- H. Associate the web ACL with the CloudFront distribution.
- I. Deploy an AWS WAF web ACL with a block default action in us-east-1. Configure an AWS WAF rate-based rule to allow matching traffic
- J. Associate the web ACL with the S3 bucket.

Answer: B

NEW QUESTION 184

- (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 188

- (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 190

- (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 191

- (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 mod
- H. Upload all files within 24 hours.

Answer: B

NEW QUESTION 192

- (Exam Topic 1)

A SysOps administrator is reviewing AWS Trusted Advisor warnings and encounters a warning for an S3 bucket policy that has open access permissions. While discussing the issue with the bucket owner, the administrator realizes the S3 bucket is an origin for an Amazon CloudFront web distribution. Which action should the administrator take to ensure that users access objects in Amazon S3 by using only CloudFront URLs?

- A. Encrypt the S3 bucket content with Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3).
- B. Create an origin access identity and grant it permissions to read objects in the S3 bucket.
- C. Assign an IAM user to the CloudFront distribution and grant the user permissions in the S3 bucket policy.
- D. Assign an IAM role to the CloudFront distribution and grant the role permissions in the S3 bucket policy.

Answer: B

Explanation:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3>

NEW QUESTION 194

- (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 195

- (Exam Topic 1)

A SysOps administrator is setting up a fleet of Amazon EC2 instances in an Auto Scaling group for an application. The fleet should have 50% CPU available at that times to accommodate bursts of traffic. The load will increase significantly between the hours of 09:00 and 17:00, 7 days a week. How should the SysOps administrator configure the scaling of the EC2 instances to meet these requirements?

- A. Create a target tracking scaling policy that runs when the CPU utilization is higher than 90%
- B. Create a target tracking scaling policy that runs when the CPU utilization is higher than 50%. Create a scheduled scaling policy that ensures that the fleet is available at 09:00. Create a second scheduled scaling policy that scales in the fleet at 17:00.
- C. Set the Auto Scaling group to start with 2 instances by setting the desired instances maximum instances, and minimum instances to 2. Create a scheduled scaling policy that ensures that the fleet is available at 09:00.
- D. Create a scheduled scaling policy that ensures that the fleet is available at 09:00. Create a second scheduled scaling policy that scales in the fleet at 17:00.

Answer: B

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 ta
- I. Tag the EC2 instances with an identifier.
- J. Create an AWS Systems Manager Automation document to remove the public IP association from the EC2 instances.

Answer: C

Explanation:

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

NEW QUESTION 201

- (Exam Topic 1)

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

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

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

Answer: C

Explanation:

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

NEW QUESTION 204

- (Exam Topic 1)

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

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

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 205

- (Exam Topic 1)

A recent audit found that most resources belonging to the development team were in violation of patch compliance standards. The resources were properly tagged. Which service should be used to quickly remediate the issue and bring the resources back into compliance?

- A. AWS Config
- B. Amazon Inspector
- C. AWS Trusted Advisor
- D. AWS Systems Manager

Answer: D

NEW QUESTION 207

- (Exam Topic 1)

A large multinational company has a core application that runs 24 hours a day, 7 days a week on Amazon EC2 and AWS Lambda. The company uses a combination of operating systems across different AWS Regions. The company wants to achieve cost savings and wants to use a pricing model that provides the most flexibility.

What should the company do to MAXIMIZE cost savings while meeting these requirements?

- A. Establish the compute expense by the hour
- B. Purchase a Compute Savings Plan.
- C. Establish the compute expense by the hour
- D. Purchase an EC2 Instance Savings Plan.
- E. Purchase a Reserved Instance for the instance types, operating systems, Region, and tenancy.
- F. Use EC2 Spot Instances to match the instances that run in each Region.

Answer: D

NEW QUESTION 211

- (Exam Topic 1)

A SysOps administrator is helping a development team deploy an application to AWS. The AWS CloudFormation template includes an Amazon Linux EC2 Instance, an Amazon Aurora DB cluster, and a hard-coded database password that must be rotated every 90 days.

What is the MOST secure way to manage the database password?

- A. Use the AWS SecretsManager Secret resource with the GenerateSecretString property to automatically generate a password. Use the AWS SecretsManager RotationSchedule resource to define a rotation schedule for the password. Configure the application to retrieve the secret from AWS Secrets Manager to access the database.
- B. Use the AWS SecretsManager Secret resource with the SecretString property. Accept a password as a CloudFormation parameter. Use the AllowedPattern property of the CloudFormation parameter to require a minimum length, uppercase and lowercase letters, and special characters. Configure the application to retrieve the secret from AWS Secrets Manager to access the database.
- C. Use the AWS SSM Parameter resource. Accept input as a CloudFormation parameter to store the parameter as a secure string. Configure the application to

retrieve the parameter from AWS Systems Manager Parameter Store to access the database

D. Use the AWS SSM Parameter resource Accept input as a CloudFormation parameter to store the parameter as a string Configure the application to retrieve the parameter from AWS Systems ManagerParameter Store to access the database

Answer: A

NEW QUESTION 215

- (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 218

- (Exam Topic 1)

A company has a web application with a database tier that consists of an Amazon EC2 instance that runs MySQL. A SysOps administrator needs to minimize potential data loss and the time that is required to recover in the event of a database failure.

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

- A. Create an Amazon CloudWatch alarm for the StatusCheckFailed_System metric to invoke an AWS Lambda function that stops and starts the EC2 instance.
- B. Create an Amazon RDS for MySQL Multi-AZ DB instance
- C. Use a MySQL native backup that is stored in Amazon S3 to restore the data to the new database
- D. Update the connection string in the web application.
- E. Create an Amazon RDS for MySQL Single-AZ DB instance with a read replica
- F. Use a MySQL native backup that is stored in Amazon S3 to restore the data to the new database
- G. Update the connection string in the web application.
- H. Use Amazon Data Lifecycle Manager (Amazon DLM) to take a snapshot of the Amazon Elastic Block Store (Amazon EBS) volume every hour
- I. In the event of an EC2 instance failure, restore the EBS volume from a snapshot.

Answer: D

NEW QUESTION 222

- (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 223

- (Exam Topic 1)

A company requires that all IAM user accounts that have not been used for 90 days or more must have their access keys and passwords immediately disabled. A SysOps administrator must automate the process of disabling unused keys using the MOST operationally efficient method.

How should the SysOps administrator implement this solution?

- A. Create an AWS Step Functions workflow to identify IAM users that have not been active for 90 days. Run an AWS Lambda function when a scheduled Amazon EventBridge (Amazon CloudWatch Events) rule is invoked to automatically remove the AWS access keys and passwords for these IAM users.
- B. Configure an AWS Config rule to identify IAM users that have not been active for 90 days. Set up an automatic weekly batch process on an Amazon EC2 instance to disable the AWS access keys and passwords for these IAM users.
- C. Develop and run a Python script on an Amazon EC2 instance to programmatically identify IAM users that have not been active for 90 days. Automatically delete these IAM users.
- D. Set up an AWS Config managed rule to identify IAM users that have not been active for 90 days. Set up an AWS Systems Manager automation runbook to disable the AWS access keys for these IAM users.

Answer: D

NEW QUESTION 225

- (Exam Topic 1)

Application A runs on Amazon EC2 instances behind a Network Load Balancer (NLB). The EC2 instances are in an Auto Scaling group and are in the same subnet that is associated with the NLB. Other applications from an on-premises environment cannot communicate with Application A on port 8080.

To troubleshoot the issue, a SysOps administrator analyzes the flow logs. The flow logs include the following records:

```
2 123456789010 eni-1235b8ca123456789 192.168.0.13 172.31.16.139 59003 8080 1 4 336 1432917027 1432917142 ACCEPT OK
2 123456789010 eni-1235b8ca123456789 172.31.16.139 192.168.0.13 8080 59003 1 4 336 1432917094 1432917142 REJECT OK
```

What is the reason for the rejected traffic?

- A. The security group of the EC2 instances has no Allow rule for the traffic from the NLB.
- B. The security group of the NLB has no Allow rule for the traffic from the on-premises environment.
- C. The ACL of the on-premises environment does not allow traffic to the AWS environment.
- D. The network ACL that is associated with the subnet does not allow outbound traffic for the ephemeral port range.

Answer: A

NEW QUESTION 228

- (Exam Topic 1)

A SysOps administrator has enabled AWS CloudTrail in an AWS account. If CloudTrail is disabled, it must be re-enabled immediately. What should the SysOps administrator do to meet these requirements WITHOUT writing custom code?

- A. Add the AWS account to AWS Organization
- B. Enable CloudTrail in the management account.
- C. Create an AWS Config rule that is invoked when CloudTrail configuration change
- D. Apply the AWS-ConfigureCloudTrailLogging automatic remediation action.
- E. Create an AWS Config rule that is invoked when CloudTrail configuration change
- F. Configure the rule to invoke an AWS Lambda function to enable CloudTrail.
- G. Create an Amazon EventBridge (Amazon CloudWatch Events) hourly rule with a schedule pattern to run an AWS Systems Manager Automation document to enable CloudTrail.

Answer: D

NEW QUESTION 233

- (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 236

- (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 239

- (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 with 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 243

- (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 248

- (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 250

- (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 252

- (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 257

- (Exam Topic 1)

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

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

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

Answer: B

Explanation:

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

NEW QUESTION 260

- (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 Report
- B. Analyze the results in Amazon Athena
- C. Configure an alarm to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic when costs reach 75% of the threshold
- 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) topic
- 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 amount
- 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 log
- 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 262

- (Exam Topic 1)

A company's customers are reporting increased latency while accessing static web content from Amazon S3. A SysOps administrator observed a very high rate of read operations on a particular S3 bucket.

What will minimize latency by reducing load on the S3 bucket?

- A. Migrate the S3 bucket to a region that is closer to end users' geographic locations
- B. Use cross-region replication to replicate all of the data to another region
- C. Create an Amazon CloudFront distribution with the S3 bucket as the origin.
- D. Use Amazon ElastiCache to cache data being served from Amazon S3

Answer: C

NEW QUESTION 264

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 269

- (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 270

- (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 encryptio
- G. Turn on S3 Cross-Region Replication on the S3 bucket.
- H. Schedule an AWS Lambda function with the Python runtim
- 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 272

- (Exam Topic 1)

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

Which solution will solve this problem?

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

Answer: C

NEW QUESTION 274

- (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 276

- (Exam Topic 1)

A SysOps administrator must ensure that a company's Amazon EC2 instances auto scale as expected. The SysOps administrator configures an Amazon EC2 Auto Scaling Lifecycle hook to send an event to Amazon EventBridge (Amazon CloudWatch Events), which then invokes an AWS Lambda function to configure the EC2 instances. When the configuration is complete, the Lambda function calls the complete Lifecycle-action event to put the EC2 instances into service. In testing, the SysOps administrator discovers that the Lambda function is not invoked when the EC2 instances auto scale.

What should the SysOps administrator do to resolve this issue?

- A. Add a permission to the Lambda function so that it can be invoked by the EventBridge (CloudWatch Events) rule.
- B. Change the lifecycle hook action to CONTINUE if the lifecycle hook experiences a failure or timeout.
- C. Configure a retry policy in the EventBridge (CloudWatch Events) rule to retry the Lambda function invocation upon failure.
- D. Update the Lambda function execution role so that it has permission to call the complete lifecycle-action event

Answer: D

NEW QUESTION 278

- (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 CloudFormation to create an Amazon EC2 instance, install a Chef server, and add Chef recipes.
- 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 281

- (Exam Topic 1)

A company is running an application on a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). The EC2 instances are launched by an Auto Scaling group and are automatically registered in a target group. A SysOps administrator must set up a notification to alert application owners when targets fail health checks.

What should the SysOps administrator do to meet these requirements?

- A. Create an Amazon CloudWatch alarm on the UnHealthyHostCount metric
- B. Configure an action to send an Amazon Simple Notification Service (Amazon SNS) notification when the metric is greater than 0.
- C. Configure an Amazon EC2 Auto Scaling custom lifecycle action to send an Amazon Simple Notification Service (Amazon SNS) notification when an instance is in the Pending:Wait state.
- D. Update the Auto Scaling group
- E. Configure an activity notification to send an Amazon Simple Notification Service (Amazon SNS) notification for the Unhealthy event type.
- F. Update the ALB health check to send an Amazon Simple Notification Service (Amazon SNS) notification when an instance is unhealthy.

Answer: A

NEW QUESTION 284

- (Exam Topic 1)

An existing, deployed solution uses Amazon EC2 instances with Amazon EBS General Purpose SSD volumes, an Amazon RDS PostgreSQL database, an Amazon EFS file system, and static objects stored in an Amazon S3 bucket. The Security team now mandates that at-rest encryption be turned on immediately for all aspects of the application, without creating new resources and without any downtime.

To satisfy the requirements, which one of these services can the SysOps administrator enable at-rest encryption on?

- A. EBS General Purpose SSD volumes
- B. RDS PostgreSQL database
- C. Amazon EFS file systems
- D. S3 objects within a bucket

Answer: D

Explanation:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingEncryption.html>

NEW QUESTION 286

- (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 289

- (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 days
- 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 293

- (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 298

- (Exam Topic 1)

An environment consists of 100 Amazon EC2 Windows instances. The Amazon CloudWatch agent is deployed and running on all EC2 instances with a baseline configuration file to capture log files. There is a new requirement to capture the DHCP log files that exist on 50 of the instances. What is the MOST operational efficient way to meet this new requirement?

- A. Create an additional CloudWatch agent configuration file to capture the DHCP logs. Use the AWS Systems Manager Run Command to restart the CloudWatch agent on each EC2 instance with the append-config option to apply the additional configuration file.
- B. Log in to each EC2 instance with administrator rights. Create a PowerShell script to push the needed baseline log files and DHCP log files to CloudWatch.
- C. Run the CloudWatch agent configuration file wizard on each EC2 instance. Verify that the base log files are included and add the DHCP log files during the wizard creation process.
- D. Run the CloudWatch agent configuration file wizard on each EC2 instance and select the advanced detail level.
- E. This will capture the operating system log files.

Answer: A

NEW QUESTION 299

- (Exam Topic 1)

A company updates its security policy to clarify cloud hosting arrangements for regulated workloads. Workloads that are identified as sensitive must run on hardware that is not shared with other customers or with other AWS accounts within the company. Which solution will ensure compliance with this policy?

- A. Deploy workloads only to Dedicated Hosts.
- B. Deploy workloads only to Dedicated Instances.
- C. Deploy workloads only to Reserved Instances.
- D. Place all instances in a dedicated placement group.

Answer: A

Explanation:

Dedicated Hosts are physical servers that are dedicated to a single customer, ensuring that the customer's workloads are not shared with other customers or with other AWS accounts within the company. This will ensure that the company's security policy is followed and that sensitive workloads are running on hardware that is not shared with other customers or with other AWS accounts within the company.

NEW QUESTION 302

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 304

- (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 306

- (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 309

- (Exam Topic 1)

A SysOps administrator creates two VPCs, VPC1 and VPC2, in a company's AWS account. The SysOps administrator deploys a Linux Amazon EC2 instance in VPC1 and deploys an Amazon RDS for MySQL DB instance in VPC2. The DB instance is deployed in a private subnet. An application that runs on the EC2 instance needs to connect to the database.

What should the SysOps administrator do to give the EC2 instance the ability to connect to the database?

- A. Enter the DB instance connection string into the VPC1 route table.
- B. Configure VPC peering between the two VPCs.
- C. Add the same IPv4 CIDR range for both VPCs.
- D. Connect to the DB instance by using the DB instance's public IP address.

Answer: B

Explanation:

VPC peering allows two VPCs to communicate with each other securely. By configuring VPC peering between the two VPCs, the SysOps administrator will be able to give the EC2 instance in VPC1 the ability to connect to the database in VPC2. Once the VPC peering is configured, the EC2 instance will be able to communicate with the database using the private IP address of the DB instance in the private subnet.

NEW QUESTION 312

- (Exam Topic 1)

A SysOps administrator is using AWS Systems Manager Patch Manager to patch a fleet of Amazon EC2 instances. The SysOps administrator has configured a patch baseline and a maintenance window. The SysOps administrator also has used an instance tag to identify which instances to patch.

The SysOps administrator must give Systems Manager the ability to access the EC2 instances. Which additional action must the SysOps administrator perform to meet this requirement?

- A. Add an inbound rule to the instances' security group.
- B. Attach an IAM instance profile with access to Systems Manager to the instances.
- C. Create a Systems Manager activation. Then activate the fleet of instances.
- D. Manually specify the instances to patch. Instead of using tag-based selection.

Answer: A

NEW QUESTION 317

- (Exam Topic 1)

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

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

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

Answer: DE

Explanation:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html

NEW QUESTION 318

- (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 320

- (Exam Topic 1)

An Amazon EC2 instance is running an application that uses Amazon Simple Queue Service (Amazon SQS) queues A SysOps administrator must ensure that the application can read, write, and delete messages from the SQS queues

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

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

Answer: D

NEW QUESTION 324

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SOA-C02 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SOA-C02 Product From:

<https://www.2passeasy.com/dumps/SOA-C02/>

Money Back Guarantee

SOA-C02 Practice Exam Features:

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