

SOA-C02 Dumps

AWS Certified SysOps Administrator - Associate (SOA-C02)

<https://www.certleader.com/SOA-C02-dumps.html>



NEW QUESTION 1

- (Exam Topic 1)

An organization with a large IT department has decided to migrate to AWS. With different job functions in the IT department, it is not desirable to give all users access to all AWS resources. Currently, the organization handles access via LDAP group membership. What is the BEST method to allow access using current LDAP credentials?

- A. Create an AWS Directory Service Simple AD. Replicate the on-premises LDAP directory to Simple AD.
- B. Create a Lambda function to read LDAP groups and automate the creation of IAM users.
- C. Use AWS CloudFormation to create IAM roles. Deploy Direct Connect to allow access to the on-premises LDAP server.
- D. Federate the LDAP directory with IAM using SAML. Create different IAM roles to correspond to different LDAP groups to limit permissions.

Answer: D

NEW QUESTION 2

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 3

- (Exam Topic 1)

A 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 4

- (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 5

- (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 6

- (Exam Topic 1)

A company stores its data in an Amazon S3 bucket. The company is required to classify the data and find any sensitive personal information in its S3 files. Which solution will meet these requirements?

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

Answer: D

Explanation:

Amazon Macie is a security service designed to help organizations find, classify, and protect sensitive data stored in Amazon S3. Amazon Macie uses machine learning to automatically discover, classify, and protect sensitive data in Amazon S3. Creating a discovery job with the managed data identifier will allow Macie to identify sensitive personal information in the S3 files and classify it accordingly. Enabling AWS Config and Amazon GuardDuty will not help with this requirement as they are not designed to automatically classify and protect data.

NEW QUESTION 7

- (Exam Topic 1)

A SysOps administrator must create a solution that immediately notifies software developers if an AWS Lambda function experiences an error. Which solution will meet this requirement?

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

Answer: A

NEW QUESTION 8

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 9

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 10

- (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 10

- (Exam Topic 1)

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

What should the SysOps administrator do to meet these requirements?

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

Answer: D

Explanation:

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

References:

- [1] <https://aws.amazon.com/fsx/>
- [2] <https://aws.amazon.com/storage/file-storage/>
- [3] <https://docs.aws.a>

NEW QUESTION 12

- (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 14

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 18

- (Exam Topic 1)

A company wants to build a solution for its business-critical Amazon RDS for MySQL database. The database requires high availability across different geographic locations. A SysOps administrator must build a solution to handle a disaster recovery (DR) scenario with the lowest recovery time objective (RTO) and recovery point objective (RPO).

Which solution meets these requirements?

- A. Create automated snapshots of the database on a schedul
- B. Copy the snapshots to the DR Region.
- C. Create a cross-Region read replica for the database.
- D. Create a Multi-AZ read replica for the database.
- E. Schedule AWS Lambda functions to create snapshots of the source database and to copy the snapshots to a DR Region.

Answer: B

NEW QUESTION 19

- (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 20

- (Exam Topic 1)

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

Which backup solution will meet these requirements?

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

Answer: D

Explanation:

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

NEW QUESTION 25

- (Exam Topic 1)

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

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

- A. a dedicated VPC.

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

Answer: C

NEW QUESTION 29

- (Exam Topic 1)

A company with multiple AWS accounts needs to obtain recommendations for AWS Lambda functions and identify optimal resource configurations for each Lambda function. How should a SysOps administrator provide these recommendations?

- A. Create an AWS Serverless Application Repository and export the Lambda function recommendations.
- B. Enable AWS Compute Optimizer and export the Lambda function recommendations
- C. Enable all features of AWS Organization and export the recommendations from AWS CloudTrailInsights.
- D. Run AWS Trusted Advisor and export the Lambda function recommendations

Answer: B

NEW QUESTION 31

- (Exam Topic 1)

A company's financial department needs to view the cost details of each project in an AWS account A SysOps administrator must perform the initial configuration that is required to view cost for each project in Cost Explorer Which solution will meet this requirement?

- A. Activate cost allocation tags Add a project tag to the appropriate resources
- B. Configure consolidated billing Create AWS Cost and Usage Reports
- C. Use AWS Budgets Create AWS Budgets reports
- D. Use cost categories to define custom groups that are based on AWS cost and usage dimensions

Answer: A

NEW QUESTION 32

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 35

- (Exam Topic 1)

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

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

Answer: B

Explanation:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/custom-tags.html> "User-defined tags are tags that you define, create, and apply to resources. After you have created and applied the user-defined tags, you can activate by using the Billing and Cost Management console for cost allocation tracking. " To meet this requirement, the SysOps administrator should activate the company-defined tags as user-defined cost allocation tags. This will ensure that the tags appear on the billing report and that the resources can be tracked with the specific tags. The other options (activating the tags as AWS generated cost allocation tags, creating a new cost category and selecting the account billing dimension, and creating a new AWS Cost and Usage Report and including the resource IDs) will not meet the requirements and are not the correct solutions for this issue.

NEW QUESTION 40

- (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 42

- (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 45

- (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 46

- (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 47

- (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 50

- (Exam Topic 1)

A company creates custom AMI images by launching new Amazon EC2 instances from an AWS CloudFormation template it installs and configure necessary software through AWS OpsWorks and takes images of each EC2 instance. The process of installing and configuring software can take between 2 to 3 hours but at times the process stalls due to installation errors.

The SysOps administrator must modify the CloudFormation template so if the process stalls, the entire stack will fail and roll back.

Based on these requirements what should be added to the template?

- A. Conditions with a timeout set to 4 hours.
- B. CreationPolicy with timeout set to 4 hours.
- C. DependsOn a timeout set to 4 hours.
- D. Metadata with a timeout set to 4 hours

Answer: B

NEW QUESTION 55

- (Exam Topic 1)

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

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

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

Answer: CD

Explanation:

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

NEW QUESTION 58

- (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 59

- (Exam Topic 1)

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

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 62

- (Exam Topic 1)

A Sysops administrator has created an Amazon EC2 instance using an AWS CloudFormation template in the us-east-I Region. The administrator finds that this

template has failed to create an EC2 instance in the us-west-2 Region. What is one cause for this failure?

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

Answer: B

Explanation:

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

NEW QUESTION 67

- (Exam Topic 1)

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

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

Answer: AC

Explanation:

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

NEW QUESTION 71

- (Exam Topic 1)

A company has mandated the use of multi-factor authentication (MFA) for all IAM users, and requires users to make all API calls using the CLI. However, users are not prompted to enter MFA tokens, and are able to run CLI commands without MFA. In an attempt to enforce MFA, the company attached an IAM policy to all users that denies API calls that have not been authenticated with MFA.

What additional step must be taken to ensure that API calls are authenticated using MFA?

- A. Enable MFA on IAM roles, and require IAM users to use role credentials to sign API calls.
- B. Ask the IAM users to log into the AWS Management Console with MFA before making API calls using the CLI.
- C. Restrict the IAM users to use of the console, as MFA is not supported for CLI use.
- D. Require users to use temporary credentials from the get-session token command to sign API calls.

Answer: D

NEW QUESTION 73

- (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 78

- (Exam Topic 1)

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

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

Answer: DE

NEW QUESTION 82

- (Exam Topic 1)

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

A couple of hours into the sale, users report slow load times and error messages for refused connections. A SysOps administrator reviews Amazon CloudWatch

metrics and notices that the CPU utilization is at 20% across the entire fleet of instances. The SysOps administrator must restore the website's functionality without making changes to the network infrastructure. Which solution will meet these requirements?

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

Answer: B

Explanation:

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

NEW QUESTION 84

- (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 88

- (Exam Topic 1)

A company wants to use only IPv6 for all its Amazon EC2 instances. The EC2 instances must not be accessible from the internet, but the EC2 instances must be able to access the internet. The company creates a dual-stack VPC and IPv6-only subnets.

How should a SysOps administrator configure the VPC to meet these requirements?

- A. Create and attach a NAT gateway
- B. Create a custom route table that includes an entry to point all IPv6 traffic to the NAT gateway
- C. Attach the custom route table to the IPv6-only subnets.
- D. Create and attach an internet gateway
- E. Create a custom route table that includes an entry to point all IPv6 traffic to the internet gateway
- F. Attach the custom route table to the IPv6-only subnets.
- G. Create and attach an egress-only internet gateway
- H. Create a custom route table that includes an entry to point all IPv6 traffic to the egress-only internet gateway
- I. Attach the custom route table to the IPv6-only subnets.
- J. Create and attach an internet gateway and a NAT gateway
- K. Create a custom route table that includes an entry to point all IPv6 traffic to the internet gateway and all IPv4 traffic to the NAT gateway
- L. Attach the custom route table to the IPv6-only subnets.

Answer: C

NEW QUESTION 91

- (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 94

- (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 95

- (Exam Topic 1)

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

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

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

Answer: AC

NEW QUESTION 99

- (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 provides additional security benefits.

NEW QUESTION 102

- (Exam Topic 1)

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

What should the SysOps administrator do to meet these requirements?

- A. Create S3 access points in Regions that are closer to the users.

- B. Create an accelerator in AWS Global Accelerator for the S3 bucket.
- C. Enable S3 Transfer Acceleration on the S3 bucket.
- D. Enable cross-origin resource sharing (CORS) on the S3 bucket.

Answer: C

Explanation:

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

NEW QUESTION 107

- (Exam Topic 1)

A company's SysOps administrator has created an Amazon EC2 instance with custom software that will be used as a template for all new EC2 instances across multiple AWS accounts. The Amazon Elastic Block Store (Amazon EBS) volumes that are attached to the EC2 instance are encrypted with AWS managed keys. The SysOps administrator creates an Amazon Machine Image (AMI) of the custom EC2 instance and plans to share the AMI with the company's other AWS accounts. The company requires that all AMIs are encrypted with AWS Key Management Service (AWS KMS) keys and that only authorized AWS accounts can access the shared AMIs.

Which solution will securely share the AMI with the other AWS accounts?

- A. In the account where the AMI was created, create a customer master key (CMK). Modify the key policy to provide kms:DescribeKey, kms:ReEncrypt, kms>CreateGrant, and kms:Decrypt permissions to the AWS accounts that the AMI will be shared with.
- B. Modify the AMI permissions to specify the AWS account numbers that the AMI will be shared with.
- C. In the account where the AMI was created, create a customer master key (CMK). Modify the key policy to provide kms:DescribeKey, kms:ReEncrypt*, kms>CreateGrant, and kms:Decrypt permissions to the AWS accounts that the AMI will be shared with.
- D. Create a copy of the AMI.
- E. and specify the CMK.
- F. Modify the permissions on the copied AMI to specify the AWS account numbers that the AMI will be shared with.
- G. In the account where the AMI was created, create a customer master key (CMK). Modify the key policy to provide kms:DescribeKey, kms:ReEncrypt, kms>CreateGrant, and kms:Decrypt permissions to the AWS accounts that the AMI will be shared with.
- H. Create a copy of the AMI.
- I. and specify the CMK.
- J. Modify the permissions on the copied AMI to make it public.
- K. In the account where the AMI was created, modify the key policy of the AWS managed key to provide kms:DescribeKey, kms:ReEncrypt, kms>CreateGrant, and kms:Decrypt permissions to the AWS accounts that the AMI will be shared with.
- L. kms:ReEncrypt, kms>CreateGrant, and kms:Decrypt permissions to the AWS accounts that the AMI will be shared with.
- M. Modify the AMI permissions to specify the AWS account numbers that the AMI will be shared with.

Answer: B

Explanation:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sharingamis-explicit.html>

NEW QUESTION 108

- (Exam Topic 1)

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

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

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

Answer: D

Explanation:

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

NEW QUESTION 113

- (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 115

- (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 118

- (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 120

- (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 122

- (Exam Topic 1)

A company is implementing a monitoring solution that is based on machine learning. The monitoring solution consumes Amazon EventBridge (Amazon CloudWatch Events) events that are generated by Amazon EC2 Auto Scaling. The monitoring solution provides detection of anomalous behavior such as unanticipated scaling events and is configured as an EventBridge (CloudWatch Events) API destination.

During initial testing, the company discovers that the monitoring solution is not receiving events. However, Amazon CloudWatch is showing that the EventBridge (CloudWatch Events) rule is being invoked. A SysOps administrator must implement a solution to retrieve client error details to help resolve this issue.

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

- A. Create an EventBridge (CloudWatch Events) archive for the event pattern to replay the event
- B. Increase the logging on the monitoring solutio
- C. Use replay to invoke the monitoring solutio
- D. Examine the error details.
- E. Add an Amazon Simple Queue Service (Amazon SQS) standard queue as a dead-letter queue for the targe
- F. Process the messages in the dead-letter queue to retrieve error details.
- G. Create a second EventBridge (CloudWatch Events) rule for the same event pattern to target an AWS Lambda functio
- H. Configure the Lambda function to invoke the monitoring solution and to record the results to Amazon CloudWatch Log
- I. Examine the errors in the logs.
- J. Configure the EventBridge (CloudWatch Events) rule to send error messages to an Amazon Simple Notification Service (Amazon SNS) topic.

Answer: A

Explanation:

"In EventBridge, you can create an archive of events so that you can easily replay them at a later time. For example, you might want to replay events to recover from errors or to validate new functionality in your application." <https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-archive.html>

NEW QUESTION 125

- (Exam Topic 1)

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

inaccessible directly from the public internet.

Public Subnet (10.0.1.0/24) Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	IGW

Private Subnet (10.0.2.0/24) Route Table

Destination	Target
10.0.0.0/16	local

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

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

Answer: B

NEW QUESTION 127

- (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 132

- (Exam Topic 1)

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

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

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

Answer: AC

NEW QUESTION 134

- (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 137

- (Exam Topic 1)

A company is using Amazon Elastic Container Service (Amazon ECS) to run a containerized application on Amazon EC2 instances. A SysOps administrator needs to monitor only traffic flows between the ECS tasks.

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

- A. Configure Amazon CloudWatch Logs on the elastic network interface of each task.
- B. Configure VPC Flow Logs on the elastic network interface of each task.
- C. Specify the awsvpc network mode in the task definition.
- D. Specify the bridge network mode in the task definition.
- E. Specify the host network mode in the task definition.

Answer: AE

NEW QUESTION 141

- (Exam Topic 1)

A company is using Amazon CloudFront to serve static content for its web application to its users. The CloudFront distribution uses an existing on-premises website as a custom origin.

The company requires the use of TLS between CloudFront and the origin server. This configuration has worked as expected for several months. However, users are now experiencing HTTP 502 (Bad Gateway) errors when they view webpages that include content from the CloudFront distribution. What should a SysOps administrator do to resolve this problem?

- A. Examine the expiration date on the certificate on the origin sit
- B. Validate that the certificate has not expire
- C. Replace the certificate if necessary.
- D. Examine the hostname on the certificate on the origin sit
- E. Validate that the hostname matches one of the hostnames on the CloudFront distributio
- F. Replace the certificate if necessary.
- G. Examine the firewall rules that are associated with the origin serve
- H. Validate that port 443 is open for inbound traffic from the interne
- I. Create an inbound rule if necessary.
- J. Examine the network ACL rules that are associated with the CloudFront distributio
- K. Validate that port 443 is open for outbound traffic to the origin serve
- L. Create an outbound rule if necessary.

Answer: A

Explanation:

HTTP 502 errors from CloudFront can occur because of the following reasons:

There's an SSL negotiation failure because the origin is using SSL/TLS protocols and ciphers that aren't supported by CloudFront.

There's an SSL negotiation failure because the SSL certificate on the origin is expired or invalid, or because the certificate chain is invalid.

There's a host header mismatch in the SSL negotiation between your CloudFront distribution and the custom origin.

The custom origin isn't responding on the ports specified in the origin settings of the CloudFront distribution. The custom origin is ending the connection to CloudFront too quickly.

<https://aws.amazon.com/premiumsupport/knowledge-center/resolve-cloudfront-connection-error/>

NEW QUESTION 142

- (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 instanc
- C. Use a MySQL native backup that is stored in Amazon S3 to restore the data to the new databas
- D. Update the connection string in the web application.
- E. Create an Amazon RDS for MySQL Single-AZ DB instance with a read replic
- F. Use a MySQL native backup that is stored in Amazon S3 to restore the data to the new databas
- 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 hou
- I. In the event of an EC2 instance failure, restore the EBS volume from a snapshot.

Answer: D

NEW QUESTION 144

- (Exam Topic 1)

A global company handles a large amount of personally identifiable information (PII) through an internal web portal. The company's application runs in a corporate data center that is connected to AWS through an AWS Direct Connect connection. The application stores the PII in Amazon S3. According to a compliance requirement, traffic from the web portal to Amazon S3 must not travel across the internet.

What should a SysOps administrator do to meet the compliance requirement?

- A. Provision an interface VPC endpoint for Amazon S3. Modify the application to use the interface endpoint.
- B. Configure AWS Network Firewall to redirect traffic to the internal S3 address.
- C. Modify the application to use the S3 path-style endpoint.
- D. Set up a range of VPC network ACLs to redirect traffic to the Internal S3 address.

Answer: B

NEW QUESTION 145

- (Exam Topic 1)

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

What should a SysOps administrator do to meet this requirement?

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

Answer: D

Explanation:

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

This will ensure that the backups are not deleted for at least 3 months after they are created. The other solutions (configuring an IAM policy that denies the

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

NEW QUESTION 149

- (Exam Topic 1)

A company is releasing a new static website hosted on Amazon S3. The static website hosting feature was enabled on the bucket and content was uploaded; however, upon navigating to the site, the following error message is received:

403 Forbidden - Access Denied

What change should be made to fix this error?

- A. Add a bucket policy that grants everyone read access to the bucket.
- B. Add a bucket policy that grants everyone read access to the bucket objects.
- C. Remove the default bucket policy that denies read access to the bucket.
- D. Configure cross-origin resource sharing (CORS) on the bucket.

Answer: B

NEW QUESTION 152

- (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 157

- (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 162

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 167

- (Exam Topic 1)

An application accesses data through a file system interface. The application runs on Amazon EC2 instances in multiple Availability Zones, all of which must share the same data. While the amount of data is currently small, the company anticipates that it will grow to tens of terabytes over the lifetime of the application.

What is the MOST scalable storage solution to fulfill this requirement?

- A. Connect a large Amazon EBS volume to multiple instances and schedule snapshots.
- B. Deploy Amazon EFS in the VPC and create mount targets in multiple subnets.
- C. Launch an EC2 instance and share data using SMB/CIFS or NFS.
- D. Deploy an AWS Storage Gateway cached volume on Amazon EC2.

Answer: B

NEW QUESTION 172

- (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 173

- (Exam Topic 1)

A SysOps administrator has Nocked public access to all company Amazon S3 buckets. The SysOps administrator wants to be notified when an S3 bucket becomes publicly readable in the future.

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

- A. Create an AWS Lambda function that periodically checks the public access settings for each S3 bucket. Set up Amazon Simple Notification Service (Amazon SNS) to send notifications.
- B. Create a cron script that uses the S3 API to check the public access settings for each S3 bucket.
- C. Set up Amazon Simple Notification Service (Amazon SNS) to send notifications.
- D. Enable S3 Event notifications for each S3 bucket.
- E. Subscribe S3 Event Notifications to an Amazon Simple Notification Service (Amazon SNS) topic.
- F. Enable the s3-bucket-public-read-prohibited managed rule in AWS Config.
- G. Subscribe the AWS Config rule to an Amazon Simple Notification Service (Amazon SNS) topic.

Answer: D

NEW QUESTION 177

- (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 178

- (Exam Topic 1)

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

Which solution will meet these requirements with the LEAST cost?

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

Answer: A

NEW QUESTION 179

- (Exam Topic 1)

A Sysops administrator creates an Amazon Elastic Kubernetes Service (Amazon EKS) cluster that uses AWS Fargate. The cluster is deployed successfully. The

Sysops administrator needs to manage the cluster by using the kubectl command line tool.

Which of the following must be configured on the Sysops administrator's machine so that kubectl can communicate with the cluster API server?

- A. The kubeconfig file
- B. The kube-proxy Amazon EKS add-on
- C. The Fargate profile
- D. The eks-connector.yaml file

Answer: A

Explanation:

The kubeconfig file is a configuration file used to store cluster authentication information, which is required to make requests to the Amazon EKS cluster API server. The kubeconfig file will need to be configured on the SysOps administrator's machine in order for kubectl to be able to communicate with the cluster API server.

<https://aws.amazon.com/blogs/developer/running-a-kubernetes-job-in-amazon-eks-on-aws-fargate-using-aws-ste>

NEW QUESTION 182

- (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 metri
- 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 grou
- 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 187

- (Exam Topic 1)

A company needs to automatically monitor an AWS account for potential unauthorized AWS Management Console logins from multiple geographic locations.

Which solution will meet this requirement?

- A. Configure Amazon Cognito to detect any compromised 1AM credentials.
- B. Set up Amazon Inspector
- C. Scan and monitor resources for unauthorized logins.
- D. Set up AWS Confi
- E. Add the iam-policy-blacklisted-check managed rule to the account.
- F. Configure Amazon GuardDuty to monitor the UnauthorizedAccess:IAMUser/ConsoleLoginSuccess finding.

Answer: D

NEW QUESTION 192

- (Exam Topic 1)

A company is planning to host its stateful web-based applications on AWS A SysOps administrator is using an Auto Scaling group of Amazon EC2 instances The web applications will run 24 hours a day 7 days a week throughout the year The company must be able to change the instance type within the same instance family later in the year based on the traffic and usage patterns

Which EC2 instance purchasing option will meet these requirements MOST cost-effectively?

- A. Convertible Reserved Instances
- B. On-Demand instances
- C. Spot instances
- D. Standard Reserved instances

Answer: A

Explanation:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ri-convertible-exchange.html>

NEW QUESTION 196

- (Exam Topic 1)

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

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

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

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

Answer: C

NEW QUESTION 197

- (Exam Topic 1)

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

Which action should be taken to meet these requirements?

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

Answer: D

NEW QUESTION 201

- (Exam Topic 1)

A company uses an Amazon Simple Queue Service (Amazon SQS) standard queue with its application. The application sends messages to the queue with unique message bodies. The company decides to switch to an SQS FIFO queue.

What must the company do to migrate to an SQS FIFO queue?

- A. Create a new SQS FIFO queue. Turn on content-based deduplication on the new FIFO queue. Update the application to include a message group ID in the messages.
- B. Create a new SQS FIFO queue. Update the application to include the DelaySeconds parameter in the messages.
- C. Modify the queue type from SQS standard to SQS FIFO. Turn off content-based deduplication on the queue. Update the application to include a message group ID in the messages.
- D. Modify the queue type from SQS standard to SQS FIFO. Update the application to send messages with identical message bodies and to include the DelaySeconds parameter in the messages.

Answer: A

Explanation:

FIFO queues don't support per-message delays, only per-queue delays. If your application sets the same value of the DelaySeconds parameter on each message, you must modify your application to remove the per-message delay and set DelaySeconds on the entire queue instead.

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues-moving.html>

NEW QUESTION 204

- (Exam Topic 1)

A SysOps Administrator is managing a web application that runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an EC2 Auto Scaling group. The administrator wants to set an alarm for when all target instances associated with the ALB are unhealthy.

Which condition should be used with the alarm?

- A. AWS/ApplicationELB HealthyHostCount <= 0
- B. AWS/ApplicationELB UnhealthyHostCount >= 1
- C. AWS/EC2 StatusCheckFailed <= 0
- D. AWS/EC2 StatusCheckFailed >= 1

Answer: A

Explanation:

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

NEW QUESTION 207

- (Exam Topic 1)

A company plans to migrate several of its high performance computing (HPC) virtual machines (VMs) to Amazon EC2 instances on AWS. A SysOps administrator must identify a placement group for this deployment. The strategy must minimize network latency and must maximize network throughput between the HPC VMs.

Which strategy should the SysOps administrator choose to meet these requirements?

- A. Deploy the instances in a cluster placement group in one Availability Zone.
- B. Deploy the instances in a partition placement group in two Availability Zones.
- C. Deploy the instances in a partition placement group in one Availability Zone.
- D. Deploy the instances in a spread placement group in two Availability Zones.

Answer: A

NEW QUESTION 212

- (Exam Topic 1)

A company hosts its website in the us-east-1 Region. The company is preparing to deploy its website into the eu-central-1 Region. Website visitors who are located in Europe should access the website that is hosted in eu-central-1. All other visitors access the website that is hosted in us-east-1. The company uses Amazon Route 53 to manage the website's DNS records.

Which routing policy should a SysOps administrator apply to the Route 53 record set to meet these requirements?

- A. Geolocation routing policy
- B. Geoproximity routing policy
- C. Latency routing policy

D. Multivalued answer routing policy

Answer: A

Explanation:

geolocation "Geolocation routing lets you choose the resources that serve your traffic based on the geographic location of your users, meaning the location that DNS queries originate from. For example, you might want all queries from Europe to be routed to an ELB load balancer in the Frankfurt region."
Could be confused with geoproximity - "Geoproximity routing lets Amazon Route 53 route traffic to your resources based on the geographic location of your users and your resources. You can also optionally choose to route more traffic or less to a given resource by specifying a value, known as a bias. A bias expands or shrinks the size of the geographic region from which traffic is routed to a resource" the use case is not needed as per question.
<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

NEW QUESTION 214

- (Exam Topic 1)

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

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

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

Answer: C

NEW QUESTION 217

- (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 220

- (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 222

- (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. D Create an internet-facing Network Load Balance
- 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 224

- (Exam Topic 1)

A company maintains a large set of sensitive data in an Amazon S3 bucket. The company's security team asks a SysOps administrator to help verify that all current objects in the S3 bucket are encrypted.

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

- A. Create a script that runs against the S3 bucket and outputs the status of each object.
- B. Create an S3 Inventory configuration on the S3 bucket to indicate the appropriate status fields.
- C. Provide the security team with an IAM user that has read access to the S3 bucket.
- D. Use the AWS CLI to output a list of all objects in the S3 bucket.

Answer: D

NEW QUESTION 225

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 229

- (Exam Topic 1)

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

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

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

Answer: D

NEW QUESTION 230

- (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 234

- (Exam Topic 1)

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

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

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

E. Use an Amazon Simple Email Service (Amazon SES) notification as an event target with an email subscription.

Answer: AD

Explanation:

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

NEW QUESTION 235

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 239

- (Exam Topic 1)

A company's VPC has connectivity to an on-premises data center through an AWS Site-to-Site VPN. The company needs Amazon EC2 instances in the VPC to send DNS queries for example.com to the DNS servers in the data center. Which solution will meet these requirements?

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

Answer: C

NEW QUESTION 243

- (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 246

- (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 249

- (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 250

- (Exam Topic 1)

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

What should a SysOps administrator do to resolve these errors?

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

Answer: B

Explanation:

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

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

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

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

NEW QUESTION 252

- (Exam Topic 1)

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

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

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

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

Answer: C

Explanation:

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

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

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

NEW QUESTION 257

- (Exam Topic 1)

A company's SysOps administrator deploys a public Network Load Balancer (NLB) in front of the company's web application. The web application does not use any Elastic IP addresses. Users must access the web application by using the company's domain name. The SysOps administrator needs to configure Amazon Route 53 to route traffic to the NLB.

Which solution will meet these requirements MOST cost-effectively?

- A. Create a Route 53 AAAA record for the NLB.

- B. Create a Route 53 alias record for the NLB.
- C. Create a Route 53 CAA record for the NLB.
- D. Create a Route 53 CNAME record for the NLB.

Answer: B

NEW QUESTION 258

- (Exam Topic 1)

A new application runs on Amazon EC2 instances and accesses data in an Amazon RDS database instance. When fully deployed in production, the application fails. The database can be queried from a console on a bastion host. When looking at the web server logs, the following error is repeated multiple times:

*** Error Establishing a Database Connection

Which of the following may be causes of the connectivity problems? (Select TWO.)

- A. The security group for the database does not have the appropriate egress rule from the database to the web server.
- B. The certificate used by the web server is not trusted by the RDS instance.
- C. The security group for the database does not have the appropriate ingress rule from the web server to the database.
- D. The port used by the application developer does not match the port specified in the RDS configuration.
- E. The database is still being created and is not available for connectivity.

Answer: CD

NEW QUESTION 262

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 264

- (Exam Topic 1)

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

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

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

Answer: B

NEW QUESTION 269

- (Exam Topic 1)

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

Which solution will give the application the ability to resolve the internal domain names?

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

Answer: B

Explanation:

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

NEW QUESTION 271

- (Exam Topic 1)

A company stores files on 50 Amazon S3 buckets in the same AWS Region. The company wants to connect to the S3 buckets securely over a private connection

from its Amazon EC2 instances. The company needs a solution that produces no additional cost. Which solution will meet these requirements?

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

Answer: C

NEW QUESTION 275

- (Exam Topic 1)

A company is testing Amazon Elasticsearch Service (Amazon ES) as a solution for analyzing system logs from a fleet of Amazon EC2 instances. During the test phase, the domain operates on a single-node cluster. A SysOps administrator needs to transition the test domain into a highly available production-grade deployment.

Which Amazon ES configuration should the SysOps administrator use to meet this requirement?

- A. Use a cluster of four data nodes across two AWS Regions
- B. Deploy four dedicated master nodes in each Region.
- C. Use a cluster of six data nodes across three Availability Zones
- D. Use three dedicated master nodes.
- E. Use a cluster of six data nodes across three Availability Zones
- F. Use six dedicated master nodes.
- G. Use a cluster of eight data nodes across two Availability Zones
- H. Deploy four master nodes in a failover AWS Region.

Answer: B

NEW QUESTION 277

- (Exam Topic 1)

A company's AWS Lambda function is experiencing performance issues. The Lambda function performs many CPU-intensive operations. The Lambda function is not running fast enough and is creating bottlenecks in the system.

What should a SysOps administrator do to resolve this issue?

- A. In the CPU launch options for the Lambda function, activate hyperthreading.
- B. Turn off the AWS managed encryption.
- C. Increase the amount of memory for the Lambda function.
- D. Load the required code into a custom layer.

Answer: C

Explanation:

Increasing the amount of memory for the Lambda function will help to improve the performance of the function. This is because the Lambda function is CPU-intensive and increasing the memory will give it access to more CPU resources and help it run faster. The other options (activating hyperthreading in the CPU launch options for the Lambda function, turning off the AWS managed encryption, and loading the required code into a custom layer) will not help to improve the performance of the Lambda function and are not the correct solutions for this issue.

<https://docs.aws.amazon.com/lambda/latest/dg/configuration-function-common.html#configuration-memory-con>

NEW QUESTION 281

- (Exam Topic 1)

A company uses AWS Organizations. A SysOps administrator wants to use AWS Compute Optimizer and AWS tag policies in the management account to govern all member accounts in the billing family. The SysOps administrator navigates to the AWS Organizations console but cannot activate tag policies through the management account.

What could be the reason for this issue?

- A. All features have not been enabled in the organization.
- B. Consolidated billing has not been enabled.
- C. The member accounts do not have tags enabled for cost allocation.
- D. The member accounts have not manually enabled trusted access for Compute Optimizer.

Answer: C

NEW QUESTION 283

- (Exam Topic 1)

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

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

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

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

Answer: B

Explanation:

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

NEW QUESTION 286

- (Exam Topic 1)

A company has an application that is deployed in two AWS Regions in an active-passive configuration. The application runs on Amazon EC2 instances behind an Application Load Balancer (ALB) in each Region. The instances are in an Amazon EC2 Auto Scaling group in each Region. The application uses an Amazon Route 53 hosted zone (or DNS). A SysOps administrator needs to configure automatic failover to the secondary Region. What should the SysOps administrator do to meet these requirements?

- A. Configure Route 53 alias records that point to each AL
- B. Choose a failover routing policy
- C. Set Evaluate Target Health to Yes.
- D. Configure CNAME records that point to each AL
- E. Choose a failover routing policy
- F. Set Evaluate Target Health to Yes.
- G. Configure Elastic Load Balancing (ELB) health checks for the Auto Scaling group
- H. Add a target group to the ALB in the primary Region
- I. Include the EC2 instances in the secondary Region as targets.
- J. Configure EC2 health checks for the Auto Scaling group
- K. Add a target group to the ALB in the primary Region
- L. Include the EC2 instances in the secondary Region as targets.

Answer: A

NEW QUESTION 291

- (Exam Topic 1)

An errant process is known to use an entire processor and run at 100%. A SysOps administrator wants to automate restarting the instance once the problem occurs for more than 2 minutes. How can this be accomplished?

- A. Create an Amazon CloudWatch alarm for the Amazon EC2 instance with basic monitoring. Enable an action to restart the instance.
- B. Create a CloudWatch alarm for the EC2 instance with detailed monitoring. Enable an action to restart the instance.
- C. Create an AWS Lambda function to restart the EC2 instance triggered on a scheduled basis every 2 minutes.
- D. Create a Lambda function to restart the EC2 instance, triggered by EC2 health checks.

Answer: B

NEW QUESTION 294

- (Exam Topic 1)

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

Which solution will meet these requirements?

- A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function when a security group change
- B. Configure the Lambda function to evaluate the security group for compliance, remove all inbound security group rules on all ports, and notify the SysOps team if the security group is noncompliant.
- C. Create an AWS CloudTrail metric filter for security group change
- D. Create an Amazon CloudWatch alarm to notify the SysOps team through an Amazon Simple Notification Service (Amazon SNS) topic when the metric is greater than 0. Subscribe an AWS Lambda function to the SNS topic to remediate the security group rule by removing the rule.
- E. Activate the AWS Config restricted-ssh managed rule
- F. Add automatic remediation to the AWS Config rule by using the AWS Systems Manager Automation AWS-DisablePublicAccessForSecurityGroup runbook
- G. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to notify the SysOps team when the rule is noncompliant.
- H. Create an AWS CloudTrail metric filter for security group change
- I. Create an Amazon CloudWatch alarm for when the metric is greater than 0. Add an AWS Systems Manager action to the CloudWatch alarm to suspend the security group by using the Systems Manager Automation AWS-DisablePublicAccessForSecurityGroup runbook when the alarm is in ALARM state
- J. Add an Amazon Simple Notification Service (Amazon SNS) topic as a second target to notify the SysOps team.

Answer: C

NEW QUESTION 298

- (Exam Topic 1)

A company migrated an I/O intensive application to an Amazon EC2 general purpose instance. The EC2 instance has a single General Purpose SSD Amazon Elastic Block Store (Amazon EBS) volume attached.

Application users report that certain actions that require intensive reading and writing to the disk are taking much longer than normal or are failing completely. After reviewing the performance metrics of the EBS volume, a SysOps administrator notices that the VolumeQueueLength metric is consistently high during the same times in which the users are reporting issues. The SysOps administrator needs to resolve this problem to restore full performance to the application.

Which action will meet these requirements?

- A. Modify the instance type to be storage optimized.
- B. Modify the volume properties by deselecting Auto-Enable Volume 10.
- C. Modify the volume properties to increase the IOPS.
- D. Modify the instance to enable enhanced networking.

Answer: C

NEW QUESTION 299

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 303

- (Exam Topic 1)

A SysOps administrator configuring AWS Client VPN to connect users on a corporate network to AWS resources that are running in a VPC. According to compliance requirements, only traffic that is destined for the VPC can travel across the VPN tunnel.

How should the SysOps administrator configure Client VPN to meet these requirements?

- A. Associate the Client VPN endpoint with a private subnet that has an internet route through a NAT gateway.
- B. On the Client VPN endpoint, turn on the split-tunnel option.
- C. On the Client VPN endpoint, specify DNS server IP addresses
- D. Select a private certificate to use as the identity certificate for the VPN client.

Answer: C

NEW QUESTION 304

- (Exam Topic 1)

A company has an Auto Scaling group of Amazon EC2 instances that scale based on average CPU utilization. The Auto Scaling group events log indicates an `InsufficientInstanceCapacity` error.

Which actions should a SysOps administrator take to remediate this issue? (Select TWO.)

- A. Change the instance type that the company is using.
- B. Configure the Auto Scaling group in different Availability Zones.
- C. Configure the Auto Scaling group to use different Amazon Elastic Block Store (Amazon EBS) volume sizes.
- D. Increase the maximum size of the Auto Scaling group.
- E. Request an increase in the instance service quota.

Answer: AB

NEW QUESTION 306

- (Exam Topic 1)

A company's SysOps administrator must ensure that all Amazon EC2 Windows instances that are launched in an AWS account have a third-party agent installed. The third-party agent has an MSI package. The company uses AWS Systems Manager for patching, and the Windows instances are tagged appropriately. The third-party agent requires periodic updates as new versions are released. The SysOps administrator must deploy these updates automatically.

Which combination of steps will meet these requirements with the LEAST operational effort? (Select TWO.) Create a Systems Manager Distributor package for the third-party agent.

- A. Make sure that Systems Manager Inventory is configured
- B. If Systems Manager Inventory is not configured, set up a new inventory for instances that is based on the appropriate tag value for Windows.
- C. Create a Systems Manager State Manager association to run the `AWS-RunRemoteScript` document. Populate the details of the third-party agent package
- D. Specify instance tags based on the appropriate tag value for Windows with a schedule of 1 day
- E. Create a Systems Manager State Manager association to run the `AWS-ConfigureAWSPackage` document
- F. Populate the details of the third-party agent package
- G. Specify instance tags based on the appropriate tag value for Windows with a schedule of 1 day
- H. Create a Systems Manager OpsItem with the tag value for Windows. Attach the Systems Manager Distributor package to the OpsItem
- I. Create a maintenance window that is specific to the package deployment. Configure the maintenance window to cover 24 hours a day.

Answer: AD

Explanation:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/distributor-working-with-packages-deploy.html>

NEW QUESTION 308

- (Exam Topic 1)

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

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

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

Answer: A

NEW QUESTION 311

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 316

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SOA-C02 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SOA-C02-dumps.html>