Exam Questions SOA-C02

AWS Certified SysOps Administrator - Associate (SOA-C02)

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

NEW QUESTION 1
- (Exam Topic 1)
A SysOps administrator has used AWS Cloud Formation to deploy a sereness application into a production VPC. The application consists of an AWS Lambda function, an Amazon DynamoOB table, and an Amazon API Gateway API. The SysOps administrator must delete the AWS Cloud Formation stack without deleting the DynamoOB table.
Which action should the SysOps administrator take before deleting the AWS Cloud Formation stack?

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

Answer: A

NEW QUESTION 2
- (Exam Topic 1)
A SysOps administrator receives an alert from Amazon GuardDuty about suspicious network activity on an Amazon EC2 instance. The GuardDuty finding lists a new external IP address as a traffic destination. The SysOps administrator does not recognize the external IP address. The SysOps administrator must block traffic to the external IP address that GuardDuty identified.
Which solution will meet this requirement?

A. Create a new security group to block traffic to the external IP addres
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 AC
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 addres
G. Assign the new security group to the entire VPC.

Answer: C

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

NEW QUESTION 3
- (Exam Topic 1)
A company has an application that is running on Amazon EC2 instances in a VPC. The application needs access to download software updates from the internet. The VPC has public subnets and private signets. The company's security policy requires all ECS instances to be deployed in private subnets
What should a SysOps administrator do to meet those requirements?

A. Add an internet gateway to the VPC In the route table for the private subnets, odd a route to the interne; gateway.
B. Add a NAT gateway to a private subne
C. In the route table for the private subnets, add a route to the NAT gateway.
D. Add a NAT gateway to a public subnet in the route table for the private subnets, add a route to the NAT gateway.
E. Add two internet gateways to the VP
F. In The route tablet for the private subnets and public subnets, add a route to each internet gateway.

Answer: C

NEW QUESTION 4
- (Exam Topic 1)
A company updates its security policy to prohibit the public exposure of any data in Amazon S3 buckets in the company's account. What should a SysOps administrator do to meet this requirement?

A. Turn on S3 Block Public Access from the account level.
B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to enforce that all S3 objects are private.
C. Use Amazon Inspector to search for S3 buckets and to automatically reset S3 ACLs if any public S3 buckets are found.
D. Use S3 Object Lambda to examine S3 ACLs and to change any public S3 ACLs to private.

Answer: A

Explanation:
Using Amazon S3 Block Public Access
as a centralized way to limit public access. Block Public Access
settings override bucket policies and object permissions. Be sure to enable Block Public Access for all accounts and buckets that you don't want publicly accessible.
https://aws.amazon.com/premiumsupport/knowledge-center/secure-s3-resources/#:~:text=Using%20Amazon%2

NEW QUESTION 5
- (Exam Topic 1)
A company creates a new member account by using AWS Organizations. A SysOps administrator needs to add AWS Business Support to the new account
Which combination of steps must the SysOps administrator take to meet this requirement? (Select TWO.)

A. Sign in to the new account by using 1AM credential
B. Change the support plan.
C. Sign in to the new account by using root user credential
D. Change the support plan.

E. Use the AWS Support API to change the support plan.
F. Reset the password of the account root user.
G. Create an IAM user that has administrator privileges in the new account.

Answer: BE

Explanation:
The best combination of steps to meet this requirement is to sign in to the new account by using root user credentials and change the support plan, and to create an IAM user that has administrator privileges in the new account.
Signing in to the new account by using root user credentials will allow the SysOps administrator to access the account and change the support plan to AWS Business Support. Additionally, creating an IAM user that has administrator privileges in the new account will ensure that the SysOps administrator has the necessary access to manage the account and make changes to the support plan if necessary.
Reference:
[1] https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_access.html#orgs_ma

NEW QUESTION 6
- (Exam Topic 1)
A SysOps administrator is provisioning an Amazon Elastic File System (Amazon EFS) file system to provide shared storage across multiple Amazon EC2 instances The instances all exist in the same VPC across multiple Availability Zones. There are two instances In each Availability Zone. The SysOps administrator must make the file system accessible to each instance with the lowest possible latency.
Which solution will meet these requirements?

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

Answer: D

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

NEW QUESTION 7
- (Exam Topic 1)
A SysOps administrator noticed that the cache hit ratio for an Amazon CloudFront distribution is less than 10%.
Which collection of configuration changes will increase the cache hit ratio for the distribution? (Select TWO.)

A. Ensure that only required cookies, query strings, and headers are forwarded in the Cache Behavior Settings.
B. Change the Viewer Protocol Policy to use HTTPS only.
C. Configure the distribution to use presigned cookies and URLs to restrict access to the distribution.
D. Enable automatic compression of objects in the Cache Behavior Settings.
E. Increase the CloudFront time to live (TTL) settings in the Cache Behavior Settings.

Answer: AE

Explanation:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cache-hit-ratio.html#cache-hit-ratio-ht

NEW QUESTION 8
- (Exam Topic 1)
A company is running a website on Amazon EC2 instances behind an Application Load Balancer (ALB). The company configured an Amazon CloudFront distribution and set the ALB as the origin. The company created an Amazon Route 53 CNAME record to send all traffic through the CloudFront distribution. As an unintended side effect, mobile users are now being served the desktop version of the website.
Which action should a SysOps administrator take to resolve this issue?

A. Configure the CloudFront distribution behavior to forward the User-Agent header.
B. Configure the CloudFront distribution origin setting
C. Add a User-Agent header to the list of origin custom headers.
D. Enable IPv6 on the AL
E. Update the CloudFront distribution origin settings to use the dualstack endpoint.
F. Enable IPv6 on the CloudFront distributio
G. Update the Route 53 record to use the dualstack endpoint.

Answer: A

Explanation:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/header-caching.html#header-caching-

NEW QUESTION 9
- (Exam Topic 1)
A company wants to track its AWS costs in all member accounts that are part of an organization in AWS Organizations. Managers of the member accounts want to

receive a notification when the estimated costs exceed a predetermined amount each month. The managers are unable to configure a billing alarm. The IAM permissions for all users are correct. What could be the cause of this issue?

A. The management/payer account does not have billing alerts turned on.
B. The company has not configured AWS Resource Access Manager (AWS RAM) to share billing information between the member accounts and the management/payer account.
C. Amazon GuardDuty is turned on for all the accounts.
D. The company has not configured an AWS Config rule to monitor billing.

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
A company has multiple AWS Site-to-Site VPN connections between a VPC and its branch offices. The company manages an Amazon Elasticsearch Service (Amazon ES) domain that is configured with public
access. The Amazon ES domain has an open domain access policy. A SysOps administrator needs to ensure that Amazon ES can be accessed only from the branch offices while preserving existing data.
Which solution will meet these requirements?

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

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
A company is partnering with an external vendor to provide data processing services. For this integration, the vendor must host the company's data in an Amazon S3 bucket in the vendor's AWS account. The vendor is allowing the company to provide an AWS Key Management Service (AWS KMS) key to encrypt the company's data. The vendor has provided an IAM role Amazon Resource Name (ARN) to the company for this integration.
What should a SysOps administrator do to configure this integration?

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

Answer: C

NEW QUESTION 15
- (Exam Topic 1)
A SysOps administrator recently configured Amazon S3 Cross-Region Replication on an S3 bucket Which of the following does this feature replicate to the destination S3 bucket by default?

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

Answer: B

NEW QUESTION 16
- (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 18
- (Exam Topic 1)
A SysOps administrator needs to create alerts that are based on the read and write metrics of Amazon Elastic Block Store (Amazon EBS) volumes that are attached to an Amazon EC2 instance. The SysOps administrator creates and enables Amazon CloudWatch alarms for the DiskReadBytes metric and the DiskWriteBytes metric.
A custom monitoring tool that is installed on the EC2 instance with the same alarm configuration indicates that the volume metrics have exceeded the threshold. However, the CloudWatch alarms were not in ALARM state.
Which action will ensure that the CloudWatch alarms function correctly?

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

Answer: A

NEW QUESTION 21
- (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 23
- (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 25
- (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 30
- (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 35
- (Exam Topic 1)
A company uses AWS Organizations to manage its AWS accounts. A SysOps administrator must create a backup strategy for all Amazon EC2 instances across all the company's AWS accounts.
Which solution will meet these requirements In the MOST operationally efficient way?

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

Answer: B

NEW QUESTION 36
- (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 38
- (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 43
- (Exam Topic 1)
A SysOps administrator is troubleshooting connection timeouts to an Amazon EC2 instance that has a public IP address. The instance has a private IP address of 172.31.16.139. When the SysOps administrator tries to ping the instance's public IP address from the remote IP address 203.0.113.12, the response is "request timed out." The flow logs contain the following information:

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

What is one cause of the problem?

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

Answer: D

NEW QUESTION 47
- (Exam Topic 1)
A SysOps administrator wants to upload a file that is 1 TB in size from on-premises to an Amazon S3 bucket using multipart uploads. What should the SysOps administrator do to meet this requirement?

A. Upload the file using the S3 console.
B. Use the s3api copy-object command.
C. Use the s3api put-object command.
D. Use the s3 cp command.

Answer: D

Explanation:
It's a best practice to use aws s3 commands (such as aws s3 cp) for multipart uploads and downloads, because these aws s3 commands automatically perform multipart uploading and downloading based on the file size. By comparison, aws s3api commands, such as aws s3api create-multipart-upload, should be used only when aws s3 commands don't support a specific upload need, such as when the multipart upload involves multiple servers, a multipart upload is manually stopped and resumed later, or when the aws s3 command doesn't support a required request parameter.
https://aws.amazon.com/premiumsupport/knowledge-center/s3-multipart-upload-cli/

NEW QUESTION 50
- (Exam Topic 1)
A company needs to upload gigabytes of files every day. The company need to achieve higher throughput and upload speeds to Amazon S3 Which action should a SysOps administrator take to meet this requirement?

A. Create an Amazon CloudFront distribution with the GET HTTP method allowed and the S3 bucket as an origin.
B. Create an Amazon ElastiCache duster and enable caching for the S3 bucket
C. Set up AWS Global Accelerator and configure it with the S3 bucket
D. Enable S3 Transfer Acceleration and use the acceleration endpoint when uploading files

Answer: D

Explanation:
Enable Amazon S3 Transfer Acceleration Amazon S3 Transfer Acceleration can provide fast and secure transfers over long distances between your client and Amazon S3. Transfer Acceleration uses Amazon CloudFront's globally distributed edge locations.
https://aws.amazon.com/premiumsupport/knowledge-center/s3-upload-large-files/

NEW QUESTION 53
- (Exam Topic 1)
A company runs a web application on three Amazon EC2 instances behind an Application Load Balancer (ALB). The company notices that random periods of increased traffic cause a degradation in the application's performance. A SysOps administrator must scale the application to meet the increased traffic.
Which solution meets these requirements?

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

Answer: C

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

NEW QUESTION 58
- (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 SiatusCheckFailedjnstance 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 addres
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 addres
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 59
- (Exam Topic 1)
A company's web application is available through an Amazon CloudFront distribution and directly through an internet-facing Application Load Balancer (ALB) A SysOps administrator must make the application accessible only through the CloudFront distribution and not directly through the ALB. The SysOps administrator must make this change without changing the application code
Which solution will meet these requirements?

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

Answer: D

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

NEW QUESTION 61
- (Exam Topic 1)
While setting up an AWS managed VPN connection, a SysOps administrator creates a customer gateway resource in AWS. The customer gateway device resides in a data center with a NAT gateway in front of it.
What address should be used to create the customer gateway resource?

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

Answer: D

NEW QUESTION 64
- (Exam Topic 1)
A company uses AWS CloudFormation to deploy its application infrastructure Recently, a user accidentally changed a property of a database in a CloudFormation template and performed a stack update that caused an interruption to the application A SysOps administrator must determine how to modify the deployment process to allow the DevOps team to continue to deploy the infrastructure, but prevent against accidental modifications to specific resources.
Which solution will meet these requirements?

A. Set up an AWS Config rule to alert based on changes to any CloudFormation stack An AWS Lambda function can then describe the stack to determine if any protected resources were modified and cancel the operation
B. Set up an Amazon CloudWatch Events event with a rule to trigger based on any CloudFormation API call An AWS Lambda function can then describe the stack to determine if any protected resources were modified and cancel the operation
C. Launch the CloudFormation templates using a stack policy with an explicit allow for all resources and an explicit deny of the protected resources with an action of Update
D. Attach an IAM policy to the DevOps team role that prevents a CloudFormation stack from updating, with a condition based on the specific Amazon Resource Names (ARNs) of the protected resources

Answer: B

NEW QUESTION 67
- (Exam Topic 1)

A SysOos administrator s tasked with analyzing database performance. The database runs on a single Amazon RDS D6 instance. The SysOps administrator finds that, during times of peak traffic, resources on the database are over utilized due to the amount of read traffic.
Which actions should the SysOps administrator take to improve RDS performance? (Select TWO.)

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

Answer: AB

NEW QUESTION 71
- (Exam Topic 1)
An organization created an Amazon Elastic File System (Amazon EFS) volume with a file system ID of
fs-85ba4Kc. and it is actively used by 10 Amazon EC2 hosts The organization has become concerned that the file system is not encrypted
How can this be resolved?

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

Answer: D

Explanation:
https://docs.aws.amazon.com/efs/latest/ug/encryption.html
Amazon EFS supports two forms of encryption for file systems, encryption of data in transit and encryption at rest. You can enable encryption of data at rest when creating an Amazon EFS file system. You can enable encryption of data in transit when you mount the file system.

NEW QUESTION 73
- (Exam Topic 1)
A SysOps administrator is unable to authenticate an AWS CLI call to an AWS service Which of the following is the cause of this issue?

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

Answer: C

NEW QUESTION 74
- (Exam Topic 1)
A company has an AWS Cloud Formation template that creates an Amazon S3 bucket. A user authenticates to the corporate AWS account with their Active Directory credentials and attempts to deploy the Cloud Formation template. However, the stack creation fails.
Which factors could cause this failure? (Select TWO.)

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

Answer: AC

NEW QUESTION 75
- (Exam Topic 1)
A company is using an Amazon Aurora MySQL DB cluster that has point-in-time recovery, backtracking, and automatic backup enabled. A SysOps administrator needs to be able to roll back the DB cluster to a specific recovery point within the previous 72 hours. Restores must be completed in the same production DB cluster.
Which solution will meet these requirements?

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

Answer: C

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

NEW QUESTION 80

- (Exam Topic 1)
A SysOps administrator is testing an application mat is hosted on five Amazon EC2 instances The instances run in an Auto Scaling group behind an Application Load Balancer (ALB) High CPU utilization during load testing is causing the Auto Scaling group to scale out. The SysOps administrator must troubleshoot to find the root cause of the high CPU utilization before the Auto Scaling group scales out.
Which action should the SysOps administrator take to meet these requirements?

A. Enable instance scale-in protection.
B. Place the instance into the Standby stale.
C. Remove the listener from the ALB
D. Suspend the Launch and Terminate process types.

Answer: A

NEW QUESTION 84
- (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 lOPs
B. Upgrade to a compute-optimized instance
C. Add additional 12 large instances to the application
D. Purchase Reserved Instances

Answer: B

NEW QUESTION 88
- (Exam Topic 1)
A company has a stateless application that is hosted on a fleet of 10 Amazon EC2 On-Demand Instances in an Auto Scaling group. A minimum of 6 instances are needed to meet service requirements.
Which action will maintain uptime for the application MOST cost-effectively?

A. Use a Spot Fleet with an On-Demand capacity of 6 instances.
B. Update the Auto Scaling group with a minimum of 6 On-Demand Instances and a maximum of 10 On-Demand Instances.
C. Update the Auto Scaling group with a minimum of 1 On-Demand Instance and a maximum of 6 On-Demand Instances.
D. Use a Spot Fleet with a target capacity of 6 instances.

Answer: A

NEW QUESTION 89
- (Exam Topic 1)
A large company is using AWS Organizations to manage its multi-account AWS environment. According to company policy, all users should have read-level access to a particular Amazon S3 bucket in a central account. The S3 bucket data should not be available outside the organization. A SysOps administrator must set up the permissions and add a bucket policy to the S3 bucket.
Which parameters should be specified to accomplish this in the MOST efficient manner?

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

Answer: A

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

NEW QUESTION 93
- (Exam Topic 1)
A company runs several workloads on AWS. The company identifies five AWS Trusted Advisor service quota metrics to monitor in a specific AWS Region. The company wants to receive email notification each time resource usage exceeds 60% of one of the service quotas.
Which solution will meet these requirements?

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

Answer: A

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

NEW QUESTION 98
- (Exam Topic 1)
A company recently acquired another corporation and all of that corporation's AWS accounts. A financial analyst needs the cost data from these accounts. A SysOps administrator uses Cost Explorer to generate cost and usage reports. The SysOps administrator notices that "No Tagkey" represents 20% of the monthly cost.
What should the SysOps administrator do to tag the "No Tagkey" resources?

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

Answer: D

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

NEW QUESTION 102
- (Exam Topic 1)
A SysOps administrator must create a solution that automatically shuts down any Amazon EC2 instances that have less than 10% average CPU utilization for 60 minutes or more.
Which solution will meet this requirement In the MOST operationally efficient manner?

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

Answer: B

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

NEW QUESTION 103
- (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 107
- (Exam Topic 1)
A company asks a SysOps administrator to ensure that AWS CloudTrail files are not tampered with after they are created. Currently, the company uses AWS Identity and Access Management (IAM) to restrict access to specific trails. The company's security team needs the ability to trace the integrity of each file.
What is the MOST operationally efficient solution that meets these requirements?

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

Answer: D

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

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

NEW QUESTION 109
- (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 114
- (Exam Topic 1)
An organization is running multiple applications for their customers. Each application is deployed by running a base AWS CloudFormation template that configures a new VPC. All applications are run in the same AWS account and AWS Region. A SysOps administrator has noticed that when trying to deploy the same AWS CloudFormation stack, it fails to deploy. What is likely to be the problem?

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

Answer: D

NEW QUESTION 115
- (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 CloudTrai
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 CloudTrai
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 117
- (Exam Topic 1)
A company manages an application that uses Amazon ElastiCache for Redis with two extra-large nodes spread across two different Availability Zones. The company's IT team discovers that the ElastiCache for Redis cluster has 75% freeable memory. The application must maintain high availability.
What is the MOST cost-effective way to resize the cluster?

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

Answer: D

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

NEW QUESTION 118
- (Exam Topic 1)
A company has a critical serverless application that uses multiple AWS Lambda functions. Each Lambda function generates 1 GB of log data daily in its own

Amazon CloudWatch Logs log group. The company's security team asks for a count of application errors, grouped by type, across all of the log groups.
What should a SysOps administrator do to meet this requirement?

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

Answer: A

NEW QUESTION 120
- (Exam Topic 1)
A company hosts a web application on an Amazon EC2 instance. The web server logs are published to Amazon CloudWatch Logs. The log events have the same structure and include the HTTP response codes that are associated with the user requests. The company needs to monitor the number of times that the web server returns an HTTP 404 response.
What is the MOST operationally efficient solution that meets these requirements?

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

Answer: A

Explanation:
This is the most operationally efficient solution that meets the requirements, as it will allow the company to monitor the number of times that the web server returns an HTTP 404 response in real-time. The other solutions (creating a CloudWatch Logs subscription filter, an AWS Lambda function, or a script) will require additional steps and resources to monitor the number of times that the web server returns an HTTP 404 response.
A metric filter allows you to search for specific terms, phrases, or values in your log events, and then to create a metric based on the number of occurrences of those search terms. This allows you to create a CloudWatch Metric that can be used to create alarms and dashboards, which can be used to monitor the number of HTTP 404 responses returned by the web server.

NEW QUESTION 122
- (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 cluste
B. Modify the application to check the cache before the application issues new queries to the databas
C. Add the results of any queries to the cache.
D. Deploy an Aurora Replica for the DB cluste
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 loa
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 applicatio
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 126
- (Exam Topic 1)
A company plans to deploy a database on an Amazon Aurora MySQL DB cluster. The database will store data for a demonstration environment. The data must be reset on a daily basis.
What is the MOST operationally efficient solution that meets these requirements?

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

Answer: D

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

NEW QUESTION 131
- (Exam Topic 1)
A company is using an Amazon DynamoDB table for data. A SysOps administrator must configure replication of the table to another AWS Region for disaster recovery.
What should the SysOps administrator do to meet this requirement?

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

Answer: C

NEW QUESTION 134
- (Exam Topic 1)
A company stores critical data m Amazon S3 buckets. A SysOps administrator must build a solution to record all S3 API activity. Which action will meet this requirement?

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

Answer: B

NEW QUESTION 135
- (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 fil
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 ke
E. Enable automatic key rotatio
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 ke
H. Enable automatic key rotatio
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 provide more control over key management and rotation and provide additional security benefits.

NEW QUESTION 138
- (Exam Topic 1)
An application runs on multiple Amazon EC2 instances in an Auto Scaling group The Auto Scaling group is
configured to use the latest version of a launch template A SysOps administrator must devise a solution that centrally manages the application logs and retains the logs for no more than 90 days
Which solution will meet these requirements?

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

Answer: C

NEW QUESTION 143
- (Exam Topic 1)
A SysOps administrator must configure a resilient tier of Amazon EC2 instances for a high performance computing (HPC) application. The HPC application requires minimum latency between nodes

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

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

Answer: AD

NEW QUESTION 144
- (Exam Topic 1)
A company uses Amazon S3 to aggregate raw video footage from various media teams across the US. The company recently expanded into new geographies in Europe and Australia. The technical teams located in Europe and Australia reported delays when uploading large video tiles into the destination S3 bucket m toe United States.
What are the MOST cost-effective ways to increase upload speeds into the S3 bucket? (Select TWO.)

A. Create multiple AWS Direct Connect connections between AWS and branch offices in Europe and Australia tor He uploads into the destination S3 bucket
B. Create multiple AWS Site-to-Site VPN connections between AWS and branch offices in Europe and Australia for file uploads into the destination S3 bucket.
C. Use Amazon S3 Transfer Acceleration for file uploads into the destination S3 bucket.
D. Use AWS Global Accelerator for file uploads into the destination S3 bucket from the branch offices in Europe and Australia.
E. Use multipart uploads for file uploads into the destination S3 bucket from the branch offices in Europe and Australia.

Answer: CE

NEW QUESTION 149
- (Exam Topic 1)
A company is storing media content in an Amazon S3 bucket and uses Amazon CloudFront to distribute the content to its users. Due to licensing terms, the company is not authorized to distribute the content in some countries. A SysOps administrator must restrict access to certain countries.
What is the MOST operationally efficient solution that meets these requirements?

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

Answer: C

NEW QUESTION 154
- (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 156
- (Exam Topic 1)
A SysOps administrator is designing a solution for an Amazon RDS for PostgreSQL DB instance. Database credentials must be stored and rotated monthly. The applications that connect to the DB instance send
write-intensive traffic with variable client connections that sometimes increase significantly in a short period of time.
Which solution should a SysOps administrator choose to meet these requirements?

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

Answer: A

NEW QUESTION 157
- (Exam Topic 1)
A SysOps administrator is reviewing AWS Trusted Advisor warnings and encounters a warning for an S3 bucket policy that has open access permissions. While discussing the issue with the bucket owner, the administrator realizes the S3 bucket is an origin for an Amazon CloudFront web distribution.
Which action should the administrator take to ensure that users access objects in Amazon S3 by using only CloudFront URLs?

A. Encrypt the S3 bucket content with Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3).
B. Create an origin access identity and grant it permissions to read objects in the S3 bucket.
C. Assign an 1AM user to the CloudFront distribution and grant the user permissions in the S3 bucket policy.
D. Assign an 1AM role to the CloudFront distribution and grant the role permissions in the S3 bucket policy.

Answer: B

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

NEW QUESTION 162
- (Exam Topic 1)
A company is creating a new multi-account architecture. A Sysops administrator must implement a login solution to centrally manage user access and permissions across all AWS accounts. The solution must be integrated with AWS Organizations and must be connected to a third-party Security Assertion Markup Language (SAML) 2.0 identity provider (IdP).
What should the SysOps administrator do to meet these requirements?

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

Answer: A

NEW QUESTION 164
- (Exam Topic 1)
A company's SysOps administrator needs to change the AWS Support plan for one of the company's AWS accounts. The account has multi-factor authentication (MFA) activated, and the MFA device is lost.
What should the SysOps administrator do to sign in?

A. Sign in as a root user by using email and phone verificatio
B. Set up a new MFA devic
C. Change the root user password.
D. Sign in as an 1AM user with administrator permission
E. Resynchronize the MFA token by using the 1AM console.
F. Sign in as an 1AM user with administrator permission
G. Reset the MFA device for the root user by adding a new device.
H. Use the forgot-password process to verify the email addres
I. Set up a new password and MFA device.

Answer: A

NEW QUESTION 167
- (Exam Topic 1)
A SysOps Administrator runs a web application that is using a microservices approach whereby different responsibilities of the application have been divided in a separate microservice running on a different Amazon EC2 instance. The administrator has been tasked with reconfiguring the infrastructure to support this approach.
How can the administrator accomplish this with the LEAST administrative overhead?

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

Answer: C

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

NEW QUESTION 169
- (Exam Topic 1)
A company runs hundreds of Amazon EC2 instances in a single AWS Region. Each EC2 instance has two attached 1 GiB General Purpose SSD (gp2) Amazon Elastic Block Store (Amazon EBS) volumes. A critical workload is using all the available IOPS capacity on the EBS volumes.
According to company policy, the company cannot change instance types or EBS volume types without completing lengthy acceptance tests to validate that the company’s applications will function properly. A SysOps administrator needs to increase the I/O performance of the EBS volumes as quickly as possible.
Which action should the SysOps administrator take to meet these requirements?

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

Answer: A

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

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

NEW QUESTION 173
- (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 174
- (Exam Topic 1)
A large multinational company has a core application that runs 24 hours a day, 7 days a week on Amazon EC2 and AWS Lambda. The company uses a combination of operating systems across different AWS Regions. The company wants to achieve cost savings and wants to use a pricing model that provides the most flexibility.
What should the company do to MAXIMIZE cost savings while meeting these requirements?

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

Answer: D

NEW QUESTION 178
- (Exam Topic 1)
A company is using an AWS KMS customer master key (CMK) with imported key material The company references the CMK by its alias in the Java application to encrypt data The CMK must be rotated every 6 months
What is the process to rotate the key?

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

Answer: B

NEW QUESTION 181
- (Exam Topic 1)
A SysOps administrator noticed that a large number of Elastic IP addresses are being created on the company's AWS account, but they are not being associated with Amazon EC2 instances, and are incurring Elastic IP address charges in the monthly bill.
How can the administrator identify who is creating the Elastic IP addresses?

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

Answer: B

NEW QUESTION 185
- (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 186
- (Exam Topic 1)
A large company is using AWS Organizations to manage its multi-account AWS environment. According to company policy, all users should have read-level access to a particular Amazon S3 bucket in a central account. The S3 bucket data should not be available outside the organization. A SysOps administrator must set up the permissions and add a bucket policy to the S3 bucket.
Which parameters should be specified to accomplish this in the MOST efficient manner?

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

Answer: C

NEW QUESTION 191
- (Exam Topic 1)
A company has a simple web application that runs on a set of Amazon EC2 instances behind an Elastic Load Balancer in the eu-west-2 Region. Amazon Route 53 holds a DNS record for the application with a simple touting policy. Users from all over the world access the application through their web browsers.
The company needs to create additional copies of the application in the us-east-1 Region and in the ap-south-1 Region. The company must direct users to the Region that provides the fastest response times when the users load the application.
What should a SysOps administrator do to meet these requirements?

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

Answer: B

NEW QUESTION 196
- (Exam Topic 1)
A company stores sensitive data in an Amazon S3 bucket. The company must log all access attempts to the S3 bucket. The company's risk team must receive immediate notification about any delete events.
Which solution will meet these requirements?

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

Answer: A

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

NEW QUESTION 199
- (Exam Topic 1)
A global company handles a large amount of personally identifiable information (Pll) 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 Pll 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 203
- (Exam Topic 1)
A company requires that all IAM user accounts that have not been used for 90 days or more must have their access keys and passwords immediately disabled A SysOps administrator must automate the process of disabling unused keys using the MOST operationally efficient method.
How should the SysOps administrator implement this solution?

A. Create an AWS Step Functions workflow to identify IAM users that have not been active for 90 days Run an AWS Lambda function when a scheduled Amazon EventBridge (Amazon CloudWatch Events) rule is invoked to automatically remove the AWS access keys and passwords for these IAM users
B. Configure an AWS Config rule to identify IAM users that have not been active for 90 days Set up an automatic weekly batch process on an Amazon EC2 instance to disable the AWS access keys and passwords for these IAM users
C. Develop and run a Python script on an Amazon EC2 instance to programmatically identify IAM users that have not been active for 90 days Automatically delete these 1AM users
D. Set up an AWS Config managed rule to identify IAM users that have not been active for 90 days Set up an AWS Systems Manager automation runbook to disable the AWS access keys for these IAM users

Answer: D

NEW QUESTION 207
- (Exam Topic 1)
Application A runs on Amazon EC2 instances behind a Network Load Balancer (NLB). The EC2 instances are in an Auto Scaling group and are in the same subnet that is associated with the NLB. Other applications from an on-premises environment cannot communicate with Application A on port 8080.
To troubleshoot the issue, a SysOps administrator analyzes the flow logs. The flow logs include the following records:

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

What is the reason for the rejected traffic?

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

Answer: A

NEW QUESTION 208
- (Exam Topic 1)
A SysOps administrator has enabled AWS CloudTrail in an AWS account. If CloudTrail is disabled, it must be re-enabled immediately. What should the SysOps administrator do to meet these requirements WITHOUT writing custom code?

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

Answer: D

NEW QUESTION 211
- (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 accoun
B. Use the organization as the source.Retrieve the compliance data from the aggregator.
C. Create an AWS Config aggregator in each accoun
D. Use an S3 bucket in an aggregator account as the destinatio
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 accoun
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 216
- (Exam Topic 1)
A development team recently deployed a new version of a web application to production. After the release, penetration testing revealed a cross-site scripting vulnerability that could expose user data.

Which AWS service will mitigate this issue?

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

Answer: A

NEW QUESTION 217
- (Exam Topic 1)
A company recently purchased Savings Plans. The company wants to receive email notification when the company's utilization drops below 90% for a given day.
Which solution will meet this requirement?

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

Answer: D

Explanation:
AWS Budgets can be used to create a Savings Plans budget and track the daily utilization of the company's Savings Plans. By creating a budget, it will trigger an action when the utilization drops below 90%, which in this case will be to send an email notification via an Amazon SNS topic. This will ensure that the company is notified when their Savings Plans utilization drops below 90%, allowing them to take action if necessary.
Reference: [1] https://docs.aws.amazon.com/savingsplans/latest/userguide/sp-usingBudgets.html

NEW QUESTION 221
- (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 225
- (Exam Topic 1)
A SysOps administrator is configuring an application on Amazon EC2 instances for a company Teams in other countries will use the application over the internet. The company requires the application endpoint to have a static pubic IP address.
How should the SysOps administrator deploy the application to meet this requirement?

A. Behind an Amazon API Gateway API
B. Behind an Application Load Balancer
C. Behind an internet-facing Network Load Balancer
D. In an Amazon CloudFront distribution

Answer: C

NEW QUESTION 229
- (Exam Topic 1)
A company's customers are reporting increased latency while accessing static web content from Amazon S3 A SysOps administrator observed a very high rate of read operations on a particular S3 bucket
What will minimize latency by reducing load on the S3 bucket?

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

Answer: C

NEW QUESTION 234
- (Exam Topic 1)
A company uses Amazon Elasticsearch Service (Amazon ES) to analyze sales and customer usage data. Members of the company's geographically dispersed sales team are traveling. They need to log in to Kibana by using their existing corporate credentials that are stored in Active Directory. The company has deployed Active Directory Federation Services (AD FS) to enable authentication to cloud services. Which solution will meet these requirements?

A. Configure Active Directory as an authentication provider in Amazon E
B. Add the Active Directory server's domain name to Amazon E

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

Answer: B

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

NEW QUESTION 238
- (Exam Topic 1)
A SysOps administrator must ensure that a company's Amazon EC2 instances auto scale as expected The SysOps administrator configures an Amazon EC2 Auto Scaling Lifecycle hook to send an event to Amazon EventBridge (Amazon CloudWatch Events), which then invokes an AWS Lambda function to configure the EC2 distances When the configuration is complete, the Lambda function calls the complete Lifecycle-action event to put the EC2 instances into service. In testing, the SysOps administrator discovers that the Lambda function is not invoked when the EC2 instances auto scale.
What should the SysOps administrator do to reserve this issue?

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

Answer: D

NEW QUESTION 241
- (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 kubect1 command line tool.
Which of the following must be configured on the Sysops administrator's machine so that kubect1 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 244
- (Exam Topic 1)
A company must migrate its applications to AWS The company is using Chef recipes for configuration management The company wants to continue to use the existing Chef recipes after the applications are migrated to AWS.
What is the MOST operationally efficient solution that meets these requirements?

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

Answer: D

NEW QUESTION 246
- (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 247
- (Exam Topic 1)
A SysOps administrator is evaluating Amazon Route 53 DNS options to address concerns about high availability for an on-premises website. The website consists of two servers: a primary active server and a secondary passive server. Route 53 should route traffic to the primary server if the associated health check returns 2xx or 3xx HTTP codes. All other traffic should be directed to the secondary passive server. The failover record type, set ID. and routing policy have been set appropriately for both primary and secondary servers.
Which next step should be taken to configure Route 53?

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

Answer: A

NEW QUESTION 251
- (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 Inspecto
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 252
- (Exam Topic 1)
An existing, deployed solution uses Amazon EC2 instances with Amazon EBS General Purpose SSD volumes, an Amazon RDS PostgreSQL database, an Amazon EFS file system, and static objects stored in an Amazon S3 bucket. The Security team now mandates that at-rest encryption be turned on immediately for all aspects of the application, without creating new resources and without any downtime.
To satisfy the requirements, which one of these services can the SysOps administrator enable at-rest encryption on?

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

Answer: D

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

NEW QUESTION 257
- (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 m 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 260
- (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 gueue 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 265
- (Exam Topic 1)
A compliance team requires all administrator passwords tor Amazon RDS DB instances to be changed at toast annually
Which solution meets this requirement in the MOST operationally efficient manned

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

Answer: A

NEW QUESTION 270
- (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 271
- (Exam Topic 1)
A company has attached the following policy to an IAM user:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "rds:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:Region": "us-east-1"
                }
            }
        },
        {
            "Effect": "Deny",
            "NotAction": [
                "ec2:*",
```

```
        {
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:Region": "us-east-1"
                }
            }
        },
        {
            "Effect": "Deny",
            "NotAction": [
                "ec2:*",
                "s3:GetObject"
            ],
            "Resource": "*"
        }
    ]
}
```

Which of the following actions are allowed for the IAM user?

A. Amazon RDS DescribeDBInstances action in the us-east-1 Region
B. Amazon S3 Putobject operation in a bucket named testbucket
C. Amazon EC2 Describe Instances action in the us-east-1 Region
D. Amazon EC2 AttachNetworkinterf ace action in the eu-west-1 Region

Answer: C

NEW QUESTION 275
- (Exam Topic 1)
A company plans to migrate several of its high performance computing (MPC) 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 Availably Zones

Answer: A

NEW QUESTION 277
- (Exam Topic 1)
A company updates its security policy to clarify cloud hosting arrangements for regulated workloads. Workloads that are identified as sensitive must run on hardware that is not shared with other customers or with other AWS accounts within the company.
Which solution will ensure compliance with this policy?

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

Answer: A

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

NEW QUESTION 278
- (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 281
- (Exam Topic 1)
A company monitors its account activity using AWS CloudTrail. and is concerned that some log files are being tampered with after the logs have been delivered to the account's Amazon S3 bucket.
Moving forward, how can the SysOps administrator confirm that the log files have not been modified after being delivered to the S3 bucket?

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

Answer: B

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

NEW QUESTION 286
- (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. Pu
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 291
- (Exam Topic 1)
A SysOps administrator created an AWS Cloud Formation template that provisions Amazon EC2 instances, an Elastic Load Balancer (ELB), and an Amazon RDS DB instance. During stack creation, the creation of the EC2 instances and the creation of the ELB are successful. However, the creation of the DB instance fails.
What is the default behavior of CloudFormation in this scenario?

A. CloudFormation will roll back the stack and delete the stack.
B. CloudFormation will roll back the stack but will not delete the stack.
C. CloudFormation will prompt the user to roll back the stack or continue.
D. CloudFormation will successfully complete the stack but will report a failed status for the DB instance.

Answer: C

NEW QUESTION 293
- (Exam Topic 1)
An AWS Lambda function is intermittently failing several times a day A SysOps administrator must find out how often this error has occurred in the last 7 days
Which action will meet this requirement in the MOST operationally efficient manner?

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

Answer: C

NEW QUESTION 296
- (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 301
- (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 functio
B. Create a new Lambda function that is named PasswordRotat
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 functio
E. Grant each Lambda function access to the KMS key so that the database password can be decrypted when require
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 databas
H. Create a Secrets Manager secret, and select the database so that Secrets Manager will use a Lambda function to update the database password automaticall
I. Specify an automatic rotation schedule of 30 day
J. Update each Lambda function to access the database password from SecretsManager.
K. Use AWS Systems Manager Parameter Store to create a secure string to store credentials for the databas
L. Create a new Lambda function called PasswordRotat
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 Stor
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 306
- (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 311
- (Exam Topic 1)
A company has a new requirement stating that all resources In AWS must be tagged according to a set policy. Which AWS service should be used to enforce and continually Identify all resources that are not in compliance with the policy?

A. AWS CloudTrail
B. Amazon Inspector
C. AWS Config
D. AWS Systems Manager

Answer: C

NEW QUESTION 312
- (Exam Topic 1)
A SysOps administrator has used AWS Cloud Formal ion to deploy a serverless application Into a production VPC. The application consists of an AWS Lambda function an Amazon DynamoDB table, and an Amazon API Gateway API. The SysOps administrator must delete the AWS Cloud Formation stack without deleting the DynamoDB table.
Which action should the SysOps administrator take before deleting the AWS Cloud Formation stack?

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

Answer: A

NEW QUESTION 316
- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 318
- (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 necessar
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 necessar
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 necessar
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 necessar
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 319
- (Exam Topic 1)
A company recently migrated its application to a VPC on AWS. An AWS Site-to-Site VPN connection connects the company’s on-premises network to the VPC. The application retrieves customer data from another system that resides on premises. The application uses an on-premises DNS server to resolve domain records. After the migration, the application is not able to connect to the customer data because of name resolution errors.
Which solution will give the application the ability to resolve the internal domain names?

A. Launch EC2 instances in the VP
B. On the EC2 instances, deploy a custom DNS forwarder that forwards all DNS requests to the on-premises DNS serve
C. Create an Amazon Route 53 private hosted zone that uses the EC2 instances for name servers.
D. Create an Amazon Route 53 Resolver outbound endpoin
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 networ
G. Set up a link aggregation group (LAG) that includes the two connection
H. Change the VPC resolver address to point to the on-premises DNS server.
I. Create an Amazon Route 53 public hosted zone for the on-premises domai
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 324
- (Exam Topic 1)
A company has a VPC with public and private subnets. An Amazon EC2 based application resides in the private subnets and needs to process raw .csv files stored in an Amazon S3 bucket. A SysOps administrator has set up the correct IAM role with the required permissions for the application to access the S3 bucket, but the application is unable to communicate with the S3 bucket.
Which action will solve this problem while adhering to least privilege access?

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

Answer: B

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

NEW QUESTION 328
- (Exam Topic 1)
A company needs to take an inventory of applications that are running on multiple Amazon EC2 instances. The company has configured users and roles with the

appropriate permissions for AWS Systems Manager. An updated version of Systems Manager Agent has been installed and is running on every instance. While configuring an inventory collection, a SysOps administrator discovers that not all the instances in a single subnet are managed by Systems Manager.
What must the SysOps administrator do to fix this issue?

A. Ensure that all the EC2 instances have the correct tags for Systems Manager access.
B. Configure AWS Identity and Access Management Access Analyzer to determine and automatically remediate the issue.
C. Ensure that all the EC2 instances have an instance profile with Systems Manager access.
D. Configure Systems Manager to use an interface VPC endpoint.

Answer: C

Explanation:
Ensuring that all the EC2 instances have an instance profile with Systems Manager access is the most effective way to fix this issue. Having an instance profile with Systems Manager access will allow the SysOps administrator to configure the inventory collection for all the instances in the subnet, regardless of whether or not they are managed by Systems Manager.

NEW QUESTION 331
- (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 EL
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 EL
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 EL
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 335
- (Exam Topic 1)
A company has an internal web application that runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group in a single Availability Zone. A SysOps administrator must make the application highly available.
Which action should the SysOps administrator take to meet this requirement?

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

Answer: C

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

NEW QUESTION 340
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

SOA-C02 Practice Exam Features:

* SOA-C02 Questions and Answers Updated Frequently

* SOA-C02 Practice Questions Verified by Expert Senior Certified Staff

* SOA-C02 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SOA-C02 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year