

# Amazon-Web-Services

## Exam Questions SOA-C02

AWS Certified SysOps Administrator - Associate (SOA-C02)



### NEW QUESTION 1

- (Exam Topic 1)

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

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

**Answer:** D

### NEW QUESTION 2

- (Exam Topic 1)

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

Which solution will meet this requirement?

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

**Answer:** C

#### Explanation:

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

### NEW QUESTION 3

- (Exam Topic 1)

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

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

**Answer:** C

### NEW QUESTION 4

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

**Answer:** A

### NEW QUESTION 5

- (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 6**

- (Exam Topic 1)

A company applies user-defined tags to resources that are associated with the company's AWS workloads. Twenty days after applying the tags, the company notices that it cannot use the tags to filter views in the AWS Cost Explorer console. What is the reason for this issue?

- A. It takes at least 30 days to be able to use tags to filter views in Cost Explorer.
- B. The company has not activated the user-defined tags for cost allocation.
- C. The company has not created an AWS Cost and Usage Report.
- D. The company has not created a usage budget in AWS Budgets.

**Answer: B**

**NEW QUESTION 7**

- (Exam Topic 1)

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

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

What is the result of this policy?

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

**Answer: B**

**NEW QUESTION 8**

- (Exam Topic 1)

A SysOps administrator must set up notifications for whenever combined billing exceeds a certain threshold for all AWS accounts within a company. The administrator has set up AWS Organizations and enabled Consolidated Billing. Which additional steps must the administrator perform to set up the billing alerts?

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

**Answer: D**

**NEW QUESTION 9**

- (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 Zone
- E. Share the directory with the other instances.
- F. Create a mount target for each instance
- G. Use each mount target to mount the EFS file system on each respective instance.
- H. Create a mount target in each Availability Zone of the VPC Use the mount target to mount the EFS file system on the Instances in the respective Availability Zone.

**Answer: D**

**Explanation:**

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

**NEW QUESTION 10**

- (Exam Topic 1)

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

Which configuration will meet these requirements?

- A. Create a failover routing policy
- B. Within the policy, configure 80% of the website traffic to be sent to the original resource
- C. Configure the remaining 20% of traffic as the failover record that points to the new resource.
- D. Create a multivalued answer routing policy
- E. Within the policy, create 4 records with the name and IP address of the original resource
- F. Configure 1 record with the name and IP address of the new resource.
- G. Create a latency-based routing policy
- H. Within the policy, configure a record pointing to the original resource with a weight of 80. Configure a record pointing to the new resource with a weight of 20.
- I. Create a weighted routing policy
- J. Within the policy, configure a weight of 80 for the record pointing to the original resource
- K. Configure a weight of 20 for the record pointing to the new resource.

**Answer: C**

**NEW QUESTION 10**

- (Exam Topic 1)

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

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

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 14**

- (Exam Topic 1)

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

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

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

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

**Answer: C**

**NEW QUESTION 19**

- (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 20

- (Exam Topic 1)

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

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

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

**Answer: C**

#### NEW QUESTION 22

- (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 24

- (Exam Topic 1)

A company recently its server infrastructure to Amazon EC2 instances. The company wants to use Amazon CloudWatch metrics to track instance memory utilization and available disk space.

What should a SysOps administrator do to meet these requirements?

- A. Configure CloudWatch from the AWS Management Console for all the instances that require monitoring by CloudWate
- B. AWS automatically installs and configures the agents for the specified instances.
- C. Install and configure the CloudWatch agent on all the instance
- D. Attach an IAM role to allow the instances to write logs to CloudWatch.
- E. Install and configure the CloudWatch agent on all the instance
- F. Attach an IAM user to allow the instances to write logs to CloudWatch.
- G. Install and configure the CloudWatch agent on all the instance
- H. Attach the necessary security groups to allow the instances to write logs to CloudWatch

**Answer: C**

#### NEW QUESTION 26

- (Exam Topic 1)

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

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

- A. Use S3 Batch Operation
- B. Specify the operation to replace all object tags.
- C. Use the AWS CLI to get the tags for each objec
- D. Save the tags in a lis
- E. Use S3 Batch Operations.Specify the operation to delete all object tag
- F. Use the AWS CLI and the list to retag the objects.
- G. Use the AWS CLI to get the tags for each objec

- H. Save the tags in a list
- I. Use the AWS CLI and the list to remove the object tag
- J. Use the AWS CLI and the list to retag the objects.
- K. Use the AWS CLI to copy the objects to another S3 bucket
- L. Add the new tag to the copied objects. Delete the original objects.

**Answer:** A

**Explanation:**

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

**NEW QUESTION 31**

- (Exam Topic 1)

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

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

**Answer:** B

**NEW QUESTION 36**

- (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 37**

- (Exam Topic 1)

A company is hosting applications on Amazon EC2 instances. The company is hosting a database on an Amazon RDS for PostgreSQL DB instance. The company requires all connections to the DB instance to be encrypted. What should a SysOps administrator do to meet this requirement?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 42**

- (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 company needs to upload gigabytes of files every day. The company needs 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 cluster 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 51**

- (Exam Topic 1)

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

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

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 53**

- (Exam Topic 1)

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

What should the SysOps administrator do to meet this requirement?

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

**Answer: B**

**Explanation:**

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

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

**NEW QUESTION 57**

- (Exam Topic 1)

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

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

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

**Answer: AB**

**NEW QUESTION 58**

- (Exam Topic 1)

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

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

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

**Answer: C**

**NEW QUESTION 60**

- (Exam Topic 1)

A software company runs a workload on Amazon EC2 instances behind an Application Load Balancer (ALB). A SysOps administrator needs to define a custom health check for the EC2 instances. What is the MOST operationally efficient solution?

- A. Set up each EC2 Instance so that it writes its healthy/unhealthy status into a shared Amazon S3 bucket for the ALB to read
- B. Configure the health check on the ALB and ensure that the HealthCheckPath setting is correct
- C. Set up Amazon ElasticCache to track the EC2 instances as they scale in and out
- D. Configure an Amazon API Gateway health check to ensure custom checks on availability of the EC2 instances

**Answer: B**

#### NEW QUESTION 65

- (Exam Topic 1)

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

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

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

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 69

- (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 Replica
- 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 70

- (Exam Topic 1)

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

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

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

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

**Answer: A**

#### NEW QUESTION 71

- (Exam Topic 1)

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

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

**Answer: CE**

**Explanation:**

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

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

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

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

**NEW QUESTION 76**

- (Exam Topic 1)

A SysOps administrator receives notification that an application that is running on Amazon EC2 instances has failed to authenticate to an Amazon RDS database. To troubleshoot, the SysOps administrator needs to investigate AWS Secrets Manager password rotation.

Which Amazon CloudWatch log will provide insight into the password rotation?

- A. AWS CloudTrail logs
- B. EC2 instance application logs
- C. AWS Lambda function logs
- D. RDS database logs

**Answer: B**

**NEW QUESTION 80**

- (Exam Topic 1)

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

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 85**

- (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 88**

- (Exam Topic 1)

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

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

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 90**

- (Exam Topic 1)

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

- A. Deploy a third-party monitoring solution to provide real-time EC2 instance monitoring
- B. List any instances with failed system status checks using the AWS Management Console
- C. Monitor AWS CloudTrail for Stopinstances API calls
- D. Review the AWS Personal Health Dashboard

**Answer:** D

**Explanation:**

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

**NEW QUESTION 93**

- (Exam Topic 1)

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

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

**Answer:** AC

**Explanation:**

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

**NEW QUESTION 96**

- (Exam Topic 1)

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

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

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

Which solution will meet these requirements?

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

**Answer:** B

**Explanation:**

[https://docs.amazonaws.cn/en\\_us/AmazonRDS/latest/AuroraUserGuide/aurora-replicas-adding.html](https://docs.amazonaws.cn/en_us/AmazonRDS/latest/AuroraUserGuide/aurora-replicas-adding.html)

**NEW QUESTION 101**

- (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 103**

- (Exam Topic 1)

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

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

- A. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the file system to the EC2 instances by using user data.
- B. Create a Multi-AZ Network Load Balancer in front of the EC2 instances.

- C. Place the EC2 instances in an Auto Scaling group within a single subnet
- D. Launch the EC2 instances into a cluster placement group
- E. Launch the EC2 instances into a partition placement group

**Answer:** AD

#### NEW QUESTION 107

- (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 in the 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 for 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 109

- (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 113

- (Exam Topic 1)

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

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

**Answer:** C

#### NEW QUESTION 115

- (Exam Topic 1)

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

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

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

**Answer:** B

#### NEW QUESTION 119

- (Exam Topic 1)

A company's SysOps administrator regularly checks the AWS Personal Health Dashboard in each of the company's accounts. The accounts are part of an organization in AWS Organizations. The company recently added 10 more accounts to the organization. The SysOps administrator must consolidate the alerts from each account's Personal Health Dashboard.

Which solution will meet this requirement with the LEAST amount of effort?

- A. Enable organizational view in AWS Health.
- B. Configure the Personal Health Dashboard in each account to forward events to a central AWS CloudTrail log.
- C. Create an AWS Lambda function to query the AWS Health API and to write all events to an Amazon DynamoDB table.
- D. Use the AWS Health API to write events to an Amazon DynamoDB table.

**Answer:** A

**Explanation:**

Enabling the organizational view in AWS Health will allow the SysOps administrator to consolidate the alerts from each account's Personal Health Dashboard. It will also provide the administrator with a single view of all the accounts in the organization, allowing them to easily monitor the health of all the accounts in the organization.

Reference:

[1] <https://aws.amazon.com/premiumsupport/knowledge-center/organizational-view-health-dashboard/>

**NEW QUESTION 121**

- (Exam Topic 1)

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

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

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

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

**Answer: C**

**NEW QUESTION 124**

- (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 Organizations. Enable CloudTrail in the management account.
- B. Create an AWS Config rule that is invoked when CloudTrail configuration changes. Apply the `AWS-ConfigureCloudTrailLogging` automatic remediation action.
- C. Create an AWS Config rule that is invoked when CloudTrail configuration changes. Configure the rule to invoke an AWS Lambda function to enable CloudTrail.
- D. 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: B**

**NEW QUESTION 129**

- (Exam Topic 1)

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

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

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

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

**Answer: A**

**NEW QUESTION 133**

- (Exam Topic 1)

A SysOps administrator is reviewing AWS Trusted Advisor warnings and encounters a warning for an S3 bucket policy that has open access permissions. While discussing the issue with the bucket owner, the administrator realizes the S3 bucket is an origin for an Amazon CloudFront web distribution.

Which action should the administrator take to ensure that users access objects in Amazon S3 by using only CloudFront URLs?

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

**Answer: B**

**Explanation:**

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

### NEW QUESTION 138

- (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 verification
- B. Set up a new MFA device
- C. Change the root user password.
- D. Sign in as an IAM user with administrator permission
- E. Resynchronize the MFA token by using the IAM console.
- F. Sign in as an IAM 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 address
- I. Set up a new password and MFA device.

**Answer:** A

### NEW QUESTION 140

- (Exam Topic 1)

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

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

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

**Answer:** C

#### Explanation:

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

### NEW QUESTION 142

- (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 146

- (Exam Topic 1)

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

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

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

- A. Create an EventBridge (CloudWatch Events) archive for the event pattern to replay the event
- B. Increase the logging on the monitoring solution
- C. Use replay to invoke the monitoring solution
- D. Examine the error details.
- E. Add an Amazon Simple Queue Service (Amazon SQS) standard queue as a dead-letter queue for the target
- F. Process the messages in the dead-letter queue to retrieve error details.

- G. Create a second EventBridge (CloudWatch Events) rule for the same event pattern to target an AWS Lambda function
- H. Configure the Lambda function to invoke the monitoring solution and to record the results to Amazon CloudWatch Log
- I. Examine the errors in the logs.
- J. Configure the EventBridge (CloudWatch Events) rule to send error messages to an Amazon Simple Notification Service (Amazon SNS) topic.

**Answer:** A

**Explanation:**

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

**NEW QUESTION 151**

- (Exam Topic 1)

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

**Public Subnet (10.0.1.0/24) Route Table**

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	IGW

**Private Subnet (10.0.2.0/24) Route Table**

Destination	Target
10.0.0.0/16	local

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

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

**Answer:** B

**NEW QUESTION 154**

- (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 158**

- (Exam Topic 1)

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

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

**Answer:** A

**NEW QUESTION 162**

- (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 site.
- B. Validate that the certificate has not expired.

- 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 166**

- (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 170**

- (Exam Topic 1)

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

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

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

**Answer: D**

**NEW QUESTION 174**

- (Exam Topic 1)

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

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

What should a SysOps administrator do to meet these requirements?

- A. In each new Region, create a new Elastic Load Balancer and a new set of EC2 Instances to run a copy of the 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 multivalued 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 175**

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 179**

- (Exam Topic 1)

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

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

**Answer: D**

**NEW QUESTION 183**

- (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 186**

- (Exam Topic 1)

A company is storing backups in an Amazon S3 bucket. The backups must not be deleted for at least 3 months after the backups are created. What should a SysOps administrator do to meet this requirement?

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

**Answer: D**

**Explanation:**

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

#### NEW QUESTION 187

- (Exam Topic 1)

A company is using Amazon Elastic File System (Amazon EFS) to share a file system among several Amazon EC2 instances. As usage increases, users report that file retrieval from the EFS file system is slower than normal.

Which action should a SysOps administrator take to improve the performance of the file system?

- A. Configure the file system for Provisioned Throughput.
- B. Enable encryption in transit on the file system.
- C. Identify any unused files in the file system, and remove the unused files.
- D. Resize the Amazon Elastic Block Store (Amazon EBS) volume of each of the EC2 instances.

**Answer: A**

#### NEW QUESTION 190

- (Exam Topic 1)

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

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

Which purchasing option will meet these requirements?

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

**Answer: C**

#### NEW QUESTION 191

- (Exam Topic 1)

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

What is a possible reason for this issue?

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

**Answer: D**

#### NEW QUESTION 194

- (Exam Topic 1)

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

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

**Answer: C**

#### NEW QUESTION 199

- (Exam Topic 1)

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

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

**Answer: C**

#### NEW QUESTION 202

- (Exam Topic 1)

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

long-running user data script that installs software. A SysOps administrator must decrease the time that is required (or new instances to become available). Which action should the SysOps administrator take to meet this requirement?

- A. Reduce the scaling thresholds so that instances are added before traffic increases
- B. Purchase Reserved Instances to cover 100% of the maximum capacity of the Auto Scaling group
- C. Update the Auto Scaling group to launch instances that have a storage optimized instance type

D. Use EC2 Image Builder to prepare an Amazon Machine Image (AMI) that has pre-installed software

**Answer:** D

**Explanation:**

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

**NEW QUESTION 205**

- (Exam Topic 1)

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

Which of the following is a cause of this?

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

**Answer:** D

**NEW QUESTION 210**

- (Exam Topic 1)

A company is using Amazon Elastic File System (Amazon EFS) to share a file system among several Amazon EC2 instances. As usage increases, users report that file retrieval from the EFS file system is slower than normal.

Which action should a SysOps administrator take to improve the performance of the file system?

- A. Configure the file system for Provisioned Throughput.
- B. Enable encryption in transit on the file system.
- C. Identify any unused files in the file system, and remove the unused files.
- D. Resize the Amazon Elastic Block Store (Amazon EBS) volume of each of the EC2 instances.

**Answer:** A

**NEW QUESTION 215**

- (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 220**

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 222**

- (Exam Topic 1)

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

Which solution will meet these requirements with the LEAST cost?

- A. Use a Provisioned IOPS SSD (Iol) Amazon Elastic Block Store (Amazon EBS) volume that is configured with 10.000 provisioned IOPS
- B. Use a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume that is configured with 10.000 provisioned IOPS.
- C. Use an Amazon Elastic File System (Amazon EFS) file system w\ Max I/O mode.
- D. Use an Amazon FSx for Windows File Server file system that is configured with 10.000 IOPS

**Answer:** A

#### NEW QUESTION 223

- (Exam Topic 1)

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

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 226

- (Exam Topic 1)

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

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

Which action will meet these requirements?

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 231

- (Exam Topic 1)

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

What should the SysOps administrator do to resolve this issue?

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

**Answer:** D

#### NEW QUESTION 232

- (Exam Topic 1)

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

Which solution will meet these requirements?

- A. Create an AWS Lambda function to call the CreateImage API operation with the EC2 instance ID and the no-reboot parameter enable
- B. Create a daily scheduled Amazon EventBridge (Amazon CloudWatch Events) rule that invokes the function.
- C. Create an AWS Lambda function to call the CreateImage API operation with the EC2 instance ID and the reboot parameter enable
- D. Create a daily scheduled Amazon EventBridge (Amazon CloudWatch Events) rule that invokes the function.

- E. Use AWS Backup to create a backup plan with a backup rule that runs dail
- F. Assign the resource ID of the EC2 instance with the no-reboot parameter enabled.
- G. Use AWS Backup to create a backup plan with a backup rule that runs dail
- H. Assign the resource ID of the EC2 instance with the reboot parameter enabled.

**Answer:** B

**Explanation:**

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

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

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

**NEW QUESTION 235**

- (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 237**

- (Exam Topic 1)

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

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

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

**Answer:** BD

**NEW QUESTION 242**

- (Exam Topic 1)

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

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

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

**Answer:** A

**Explanation:**

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

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

**NEW QUESTION 244**

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 249**

- (Exam Topic 1)

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

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

- A. Geolocation routing policy
- B. Geoproximity routing policy
- C. Latency routing policy
- D. Multivalue answer routing policy

**Answer:** A

**Explanation:**

geolocation "Geolocation routing lets you choose the resources that serve your traffic based on the geographic location of your users, meaning the location that DNS queries originate from. For example, you might want all queries from Europe to be routed to an ELB load balancer in the Frankfurt region."

Could be confused with geoproximity - "Geoproximity routing lets Amazon Route 53 route traffic to your resources based on the geographic location of your users and your resources. You can also optionally choose to route more traffic or less to a given resource by specifying a value, known as a bias. A bias expands or shrinks the size of the geographic region from which traffic is routed to a resource" the use case is not needed as per question.

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

**NEW QUESTION 253**

- (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 258**

- (Exam Topic 1)

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

How can this requirement be met?

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

**Answer:** C

**NEW QUESTION 263**

- (Exam Topic 1)

A team of On-call engineers frequently needs to connect to Amazon EC2 Instances in a private subnet to troubleshoot and run commands. The Instances use either the latest AWS-provided Windows Amazon Machine Images (AMIs) or Amazon Linux AMIs.

The team has an existing IAM role for authorization. A SysOps administrator must provide the team with access to the Instances by granting IAM permissions to this Which solution will meet this requirement?

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

**Answer:** A

**NEW QUESTION 267**

- (Exam Topic 1)

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

current objects in the S3 bucket are encrypted.

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

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

**Answer: D**

#### NEW QUESTION 268

- (Exam Topic 1)

A company is managing multiple AWS accounts in AWS Organizations. The company is reviewing internal security of its AWS environment. The company's security administrator has their own AWS account and wants to review the VPC configuration of developer AWS accounts. Which solution will meet these requirements in the MOST secure manner?

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

**Answer: D**

#### NEW QUESTION 271

- (Exam Topic 1)

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

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 276

- (Exam Topic 1)

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

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

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

**Answer: AD**

#### Explanation:

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

#### NEW QUESTION 279

- (Exam Topic 1)

A SysOps administrator created an AWS CloudFormation 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 284

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

**Answer: C**

#### NEW QUESTION 286

- (Exam Topic 1)

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

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

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

**Answer: A**

#### NEW QUESTION 287

- (Exam Topic 1)

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

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

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

**Answer: DE**

#### Explanation:

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

#### NEW QUESTION 290

- (Exam Topic 1)

A company using AWS Organizations requires that no Amazon S3 buckets in its production accounts should ever be deleted.

What is the SIMPLEST approach the SysOps administrator can take to ensure S3 buckets in those accounts can never be deleted?

- A. Set up MFA Delete on all the S3 buckets to prevent the buckets from being deleted.
- B. Use service control policies to deny the s3:DeleteBucket action on all buckets in production accounts.
- C. Create an IAM group that has an IAM policy to deny the s3:DeleteBucket action on all buckets in production accounts.
- D. Use AWS Shield to deny the s3:DeleteBucket action on the AWS account instead of all S3 buckets.

**Answer: B**

#### Explanation:

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scps.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html)

If you're using AWS Organizations, check the service control policies for any statements that explicitly deny Amazon S3 access. In particular, check the service control policies for statements denying the s3:PutBucketPolicy action.

<https://aws.amazon.com/tw/premiumsupport/knowledge-center/s3-access-denied-bucket-policy/>

#### NEW QUESTION 293

- (Exam Topic 1)

A SysOps administrator is responsible for a company's security groups. The company wants to maintain a documented trail of any changes that are made to the security groups. The SysOps administrator must receive notification whenever the security groups change.

Which solution will meet these requirements?

- A. Set up Amazon Detective to record security group change
- B. Specify an Amazon CloudWatch Logs log group to store configuration history log
- C. Create an Amazon Simple Queue Service (Amazon SQS) queue for notifications about configuration change
- D. Subscribe the SysOps administrator's email address to the SQS queue.
- E. Set up AWS Systems Manager Change Manager to record security group change
- F. Specify an Amazon CloudWatch Logs log group to store configuration history log

- G. Create an Amazon Simple Notification Service (Amazon SNS) topic for notifications about configuration change
- H. Subscribe the SysOps administrator's email address to the SNS topic.
- I. Set up AWS Config to record security group change
- J. Specify an Amazon S3 bucket as the location for configuration snapshots and history file
- K. Create an Amazon Simple Notification Service (Amazon SNS) topic for notifications about configuration change
- L. Subscribe the SysOps administrator's email address to the SNS topic.
- M. Set up Amazon Detective to record security group change
- N. Specify an Amazon S3 bucket as the location for configuration snapshots and history file
- O. Create an Amazon Simple Notification Service (Amazon SNS) topic for notifications about configuration change
- P. Subscribe the SysOps administrator's email address to the SNS topic.

**Answer: D**

#### NEW QUESTION 297

- (Exam Topic 1)

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

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

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

**Answer: A**

#### NEW QUESTION 299

- (Exam Topic 1)

A company has an initiative to reduce costs associated with Amazon EC2 and AWS Lambda. Which action should a SysOps administrator take to meet these requirements?

- A. Analyze the AWS Cost and Usage Report by using Amazon Athena to identify cost savings.
- B. Create an AWS Budgets alert to alarm when account spend reaches 80% of the budget.
- C. Purchase Reserved Instances through the Amazon EC2 console.
- D. Use AWS Compute Optimizer and take action on the provided recommendations.

**Answer: D**

#### NEW QUESTION 302

- (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 306

- (Exam Topic 1)

A SysOps administrator needs to design a high-traffic static website. The website must be highly available and must provide the lowest possible latency to users across the globe.

Which solution will meet these requirements?

- A. Create an Amazon S3 bucket, and upload the website content to the S3 bucket
- B. Create an Amazon CloudFront distribution in each AWS Region, and set the S3 bucket as the origin
- C. Use Amazon Route 53 to create a DNS record that uses a geolocation routing policy to route traffic to the correct CloudFront distribution based on where the request originates.
- D. Create an Amazon S3 bucket, and upload the website content to the S3 bucket
- E. Create an Amazon CloudFront distribution, and set the S3 bucket as the origin
- F. Use Amazon Route 53 to create an alias record that points to the CloudFront distribution.
- G. Create an Application Load Balancer (ALB) and a target group
- H. Create an Amazon EC2 Auto Scaling group with at least two EC2 instances in the associated target group
- I. Store the website content on the EC2 instance
- J. Use Amazon Route 53 to create an alias record that points to the ALB.
- K. Create an Application Load Balancer (ALB) and a target group in two Regions
- L. Create an Amazon EC2 Auto Scaling group in each Region with at least two EC2 instances in each target group
- M. Store the website content on the EC2 instance
- N. Use Amazon Route 53 to create a DNS record that uses a geolocation routing policy to route traffic to the correct ALB based on where the request originates.

**Answer: B**

### NEW QUESTION 309

- (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 313

- (Exam Topic 1)

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

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

**Answer: D**

### NEW QUESTION 314

- (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 315

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

**Answer: B**

#### Explanation:

[https://docs.aws.amazon.com/zh\\_tw/Route53/latest/DeveloperGuide/resolver-forwarding-outbound-queries.html](https://docs.aws.amazon.com/zh_tw/Route53/latest/DeveloperGuide/resolver-forwarding-outbound-queries.html)

### NEW QUESTION 320

- (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 VPC
- 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 324

- (Exam Topic 1)

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

What should a SysOps administrator do to resolve this issue?

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

**Answer: C**

#### Explanation:

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

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

#### NEW QUESTION 327

- (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 329

- (Exam Topic 1)

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

Which solution will meet these requirements?

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

**Answer: C**

#### NEW QUESTION 330

- (Exam Topic 1)

A SysOps administrator is tasked with deploying a company's infrastructure as code. The SysOps administrator wants to write a single template that can be reused for multiple environments.

How should the SysOps administrator use AWS CloudFormation to create a solution?

- A. Use Amazon EC2 user data in a CloudFormation template
- B. Use nested stacks to provision resources
- C. Use parameters in a CloudFormation template

D. Use stack policies to provision resources

**Answer: C**

**Explanation:**

Reuse templates to replicate stacks in multiple environments After you have your stacks and resources set up, you can reuse your templates to replicate your infrastructure in multiple environments. For example, you can create environments for development, testing, and production so that you can test changes before implementing them into production. To make templates reusable, use the parameters, mappings, and conditions sections so that you can customize your stacks when you create them. For example, for your development environments, you can specify a lower-cost instance type compared to your production environment, but all other configurations and settings remain the same. <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/best-practices.html#reuse>

**NEW QUESTION 332**

- (Exam Topic 1)

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

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

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

**Answer: C**

**NEW QUESTION 334**

- (Exam Topic 1)

A SysOps administrator developed a Python script that uses the AWS SDK to conduct several maintenance tasks. The script needs to run automatically every night.

What is the MOST operationally efficient solution that meets this requirement?

- A. Convert the Python script to an AWS Lambda (unconfined) function.
- B. Use an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke the function every night.
- C. Convert the Python script to an AWS Lambda function.
- D. Use AWS CloudTrail to invoke the function every night.
- E. Deploy the Python script to an Amazon EC2 Instance.
- F. Use Amazon EventBridge (Amazon CloudWatch Events) to schedule the instance to start and stop every night.
- G. Deploy the Python script to an Amazon EC2 instance.
- H. Use AWS Systems Manager to schedule the instance to start and stop every night.

**Answer: A**

**NEW QUESTION 336**

- (Exam Topic 1)

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

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

**Answer: D**

**NEW QUESTION 341**

- (Exam Topic 1)

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

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

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

**Answer: C**

**NEW QUESTION 346**

.....

## **Thank You for Trying Our Product**

### **We offer two products:**

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### **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 First Try
- \* SOA-C02 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The SOA-C02 Practice Test Here](#)**