

AWS Certified SysOps Administrator – Associate.VCEplus.premium.exam.54q

Number: SOA-C02
Passing Score: 800
Time Limit: 120 min
File Version: 1.0



Website: <https://vceplus.com> - <https://vceplus.co>
VCE to PDF Converter: <https://vceplus.com/vce-to-pdf/>
Facebook: <https://www.facebook.com/VCE.For.All.VN/>
Twitter : https://twitter.com/VCE_Plus

SOA-C02

AWS Certified SysOps Administrator – Associate (Beta)



Exam A

QUESTION 1

A SysOps administrator is creating two AWS CloudFormation templates. The first template will create a VPC with associated resources, such as subnets, route tables, and an internet gateway. The second template will deploy application resources within the VPC that was created by the first template. The second template should refer to the resources created by the first template.

How can this be accomplished with the LEAST amount of administrative effort?

- A. Add an export field to the outputs of the first template and import the values in the second template.
- B. Create a custom resource that queries the stack created by the first template and retrieves the required values.
- C. Create a mapping in the first template that is referenced by the second template.
- D. Input the names of resources in the first template and refer to those names in the second template as a parameter.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

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.



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

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

Which backup solution will meet these requirements?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

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

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

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

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

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

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

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

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

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 9

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 for 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.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

A company needs to restrict access to an Amazon S3 bucket to Amazon EC2 instances in a VPC only. All traffic must be over the AWS private network.

What actions should the SysOps administrator take to meet these requirements?

- A. Create a VPC endpoint for the S3 bucket, and create an IAM policy that conditionally limits all S3 actions on the bucket to the VPC endpoint as the source.

- B. Create a VPC endpoint for the S3 bucket, and create an S3 bucket policy that conditionally limits all S3 actions on the bucket to the VPC endpoint as the source.
- C. Create a service-linked role for Amazon EC2 that allows the EC2 instances to interact directly with Amazon S3, and attach an IAM policy to the role that allows the EC2 instances full access to the S3 bucket.
- D. Create a NAT gateway in the VPC, and modify the VPC route table to route all traffic destined for Amazon S3 through the NAT gateway.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

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

Where can the administrator find this information?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-dg.pdf> (206)

QUESTION 12

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://aws.amazon.com/premiumsupport/knowledge-center/aurora-mysql-slow-snapshot-restore/>

QUESTION 13

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

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

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

Which solution will meet these requirements?

- A. Activate unlimited mode for the instances in the Auto Scaling group.

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/burstable-performance-instances-how-to.html>

QUESTION 14

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

Which solution will meet these requirements?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://aws.amazon.com/blogs/security/how-to-enable-secure-access-to-kibana-using-aws-single-sign-on/>

QUESTION 15 An Amazon EC2 instance is running an application that uses Amazon Simple Queue Service (Amazon SQS) queues. A SysOps administrator must ensure that the application can read, write, and delete messages from the SQS queues.

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

A company has an internal web application that runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group in a single Availability Zone. A SysOps administrator must make the application highly available.

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

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

What should the SysOps administrator do to meet these requirements?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 18

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

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

- A. Request a public certificate by using AWS Certificate Manager (ACM). Associate the certificate from ACM with the ELB. Write a scheduled AWS Lambda function to renew the certificate every 18 months.
- B. Request a public certificate by using AWS Certificate Manager (ACM). Associate the certificate from ACM with the ELB. ACM will automatically manage the renewal of the certificate.
- C. Register a certificate with a third-party certificate authority (CA). Import this certificate into AWS Certificate Manager (ACM). Associate the certificate from ACM with the ELB. ACM will automatically manage the renewal of the certificate.
- D. Register a certificate with a third-party certificate authority (CA). Configure the ELB to import the certificate directly from the CA. Set the certificate refresh cycle on the ELB to refresh when the certificate is within 3 months of the expiration date.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

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. Configure the route table for the private subnet.
- C. Configure the route table to allow the instances on the private subnet access through the internet gateway.
- D. Create a NAT Gateway in a private subnet and configure the route table for the private subnets.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:**QUESTION 20**

A company hosts a website on multiple Amazon EC2 instances that run in an Auto Scaling group. Users are reporting slow responses during peak times between 6 PM and 11 PM every weekend. A SysOps administrator must implement a solution to improve performance during these peak times.

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

- A. Create a scheduled Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function to increase the desired capacity before peak times.
- B. Configure a scheduled scaling action with a recurrence option to change the desired capacity before and after peak times.
- C. Create a target tracking scaling policy to add more instances when memory utilization is above 70%.
- D. Configure the cooldown period for the Auto Scaling group to modify desired capacity before and after peak times.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:**QUESTION 21**

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

Which condition should be used with the alarm?

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



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:**QUESTION 22**

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

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>

QUESTION 23

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

What should the SysOps administrator do to remediate the consistently high PercentIOLimit metric?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

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.

Correct Answer: C

Section: (none)

Explanation



Explanation/Reference:

Reference: <https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-transition-general-considerations.html>

QUESTION 25

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.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

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

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

- A. Create a CNAME record. Enter static.cloudfront.net as the record name. Enter the CloudFront distribution's public IP address as the value.

- B. Create a CNAME record. Enter static.example.com as the record name. Enter the CloudFront distribution's private IP address as the value.
- C. Create an A record. Enter static.cloudfront.net as the record name. Enter the CloudFront distribution's ID as an alias target.
- D. Create an A record. Enter static.example.com as the record name. Enter the CloudFront distribution's domain name as an alias target.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 27

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.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

A company is running a website on Amazon EC2 instances behind an Application Load Balancer (ALB). The company configured an Amazon CloudFront distribution and set the ALB as the origin. The company created an Amazon Route 53 CNAME record to send all traffic through the CloudFront distribution. As an unintended side effect, mobile users are now being served the desktop version of the website.

Which action should a SysOps administrator take to resolve this issue?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-elb-load-balancer.html>

QUESTION 29

A company hosts its website on Amazon EC2 instances behind an Application Load Balancer. The company manages its DNS with Amazon Route 53, and wants to point its domain's zone apex to the website.

Which type of record should be used to meet these requirements?

- A. An AAAA record for the domain's zone apex
- B. An A record for the domain's zone apex
- C. A CNAME record for the domain's zone apex
- D. An alias record for the domain's zone apex

Correct Answer: D

Section: (none)

Explanation**Explanation/Reference:**

Reference: <https://aws.amazon.com/route53/faqs/>

QUESTION 30

A SysOps administrator is maintaining a web application using an Amazon CloudFront web distribution, an Application Load Balancer (ALB), Amazon RDS, and Amazon EC2 in a VPC. All services have logging enabled. The administrator needs to investigate HTTP Layer 7 status codes from the web application.

Which log sources contain the status codes? (Choose two.)

- A. VPC Flow Logs
- B. AWS CloudTrail logs
- C. ALB access logs
- D. CloudFront access logs
- E. RDS logs

Correct Answer: CD

Section: (none)

Explanation**Explanation/Reference:****QUESTION 31**

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.



Correct Answer: DE

Section: (none)

Explanation**Explanation/Reference:****QUESTION 32**

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

What is likely to be the problem?

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

Correct Answer: D

Section: (none)

Explanation**Explanation/Reference:**

Reference: <https://docs.aws.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html>

QUESTION 33

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 master account as the principal.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://aws.amazon.com/blogs/security/iam-share-aws-resources-groups-aws-accounts-aws-organizations/>

QUESTION 34

An Amazon S3 Inventory report reveals that more than 1 million objects in an S3 bucket are not encrypted. These objects must be encrypted, and all future objects must be encrypted at the time they are written.

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

- A. Create an AWS Config rule that runs evaluations against configuration changes to the S3 bucket. When an unencrypted object is found, run an AWS Systems Manager Automation document to encrypt the object in place.
- B. Edit the properties of the S3 bucket to enable default server-side encryption.
- C. Filter the S3 Inventory report by using S3 Select to find all objects that are not encrypted. Create an S3 Batch Operations job to copy each object in place with encryption enabled.
- D. Filter the S3 Inventory report by using S3 Select to find all objects that are not encrypted. Send each object name as a message to an Amazon Simple Queue Service (Amazon SQS) queue. Use the SQS queue to invoke an AWS Lambda function to tag each object with a key of "Encryption" and a value of "SSE-KMS".
- E. Use S3 Event Notifications to invoke an AWS Lambda function on all new object-created events for the S3 bucket. Configure the Lambda function to check whether the object is encrypted and to run an AWS Systems Manager Automation document to encrypt the object in place when an unencrypted object is found.

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 35 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.

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.aws.amazon.com/AmazonS3/latest/userguide/acl-overview.html#sample-acl>

QUESTION 36

A SysOps administrator is notified that an Amazon EC2 instance has stopped responding. The AWS Management Console indicates that the system checks are failing.

What should the administrator do first to resolve this issue?

- A. Reboot the EC2 instance so it can be launched on a new host.
- B. Stop and then start the EC2 instance so that it can be launched on a new host.
- C. Terminate the EC2 instance and relaunch it.
- D. View the AWS CloudTrail log to investigate what changed on the EC2 instance.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 37

An organization created an Amazon Elastic File System (Amazon EFS) volume with a file system ID of fs-85ba41fc, and it is actively used by 10 Amazon EC2 hosts. The organization has become concerned that the file system is not encrypted.

How can this be resolved?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 38

A company hosts a web application on an Amazon EC2 instance in a production VPC. Client connections to the application are failing. A SysOps administrator inspects the VPC flow logs and finds the following entry:

```
2 111122223333 eni-<###> 192.0.2.15 203.0.113.56 40711 443 6 1 40 1418530010 1418530070 REJECT OK
```

What is a possible cause of these failed connections?

- A. A security group is denying traffic on port 443.
- B. The EC2 instance is shut down.
- C. The network ACL is blocking HTTPS traffic.
- D. The VPC has no internet gateway attached.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

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

Which solution will net these requirements?

- A. Create a single AWS Storage Gateway file gateway.
- B. Create an Amazon FSx for Windows File Server Multi-AZ file system.
- C. Deploy two AWS Storage Gateway file gateways across two Availability Zones. Configure an Application Load Balancer in front of the file gateways.

D. Deploy two Amazon FSx for Windows File Server Single-AZ 2 file systems. Configure Microsoft Distributed File System Replication (DFSR).

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.aws.amazon.com/fsx/latest/WindowsGuide/what-is.html>

QUESTION 40

A new website will run on Amazon EC2 instances behind an Application Load Balancer. Amazon Route 53 will be used to manage DNS records.

What type of record should be set in Route 53 to point the website's apex domain name (for example, "company.com") to the Application Load Balancer?

- A. CNAME
- B. SOA
- C. TXT
- D. ALIAS

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.aws.amazon.com/govcloud-us/latest/UserGuide/setting-up-route53-zoneapex-elb.html>

QUESTION 41

A company's SysOps administrator has created an Amazon EC2 instance with custom software that will be used as a template for all new EC2 instances across multiple AWS accounts. The Amazon Elastic Block Store (Amazon EBS) volumes that are attached to the EC2 instance are encrypted with AWS managed keys.

The SysOps administrator creates an Amazon Machine Image (AMI) of the custom EC2 instance and plans to share the AMI with the company's other AWS accounts. The company requires that all AMIs are encrypted with AWS Key Management Service (AWS KMS) keys and that only authorized AWS accounts can access the shared AMIs.

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 42

A company has a stateful web application that is hosted on Amazon EC2 instances in an Auto Scaling group. The instances run behind an Application Load Balancer (ALB) that has a single target group. The ALB is configured as the origin in an Amazon CloudFront distribution. Users are reporting random logouts from the web application. Which combination of actions should a SysOps administrator take to resolve this problem? (Choose two.)

- A. Change to the least outstanding requests algorithm on the ALB target group.
- B. Configure cookie forwarding in the CloudFront distribution cache behavior.
- C. Configure header forwarding in the CloudFront distribution cache behavior.
- D. Enable group-level stickiness on the ALB listener rule.

E. Enable sticky sessions on the ALB target group.

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 43

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 enabled. Create a daily scheduled Amazon EventBridge (Amazon CloudWatch Events) rule that invokes thefunction.
- B. Create an AWS Lambda function to call the CreateImage API operation with the EC2 instance ID and the reboot parameter enabled. Create a daily scheduled Amazon EventBridge (Amazon CloudWatch Events) rule that invokes thefunction.
- C. Use AWS Backup to create a backup plan with a backup rule that runs daily. Assign the resource ID of the EC2 instance with the no-reboot parameter enabled.
- D. Use AWS Backup to create a backup plan with a backup rule that runs daily. Assign the resource ID of the EC2 instance with the reboot parameter enabled.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 44

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.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 45

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

Which solution will meet these requirements?

- A. Create an Amazon CloudWatch alarm for the EC2 instance, and specify the StatusCheckFailed_Instance metric. Add an EC2 action to the alarm to recover the instance. Add an alarm notification to publish a message to an AmazonSimple Notification Service (Amazon SNS) topic. Subscribe the SysOps team email address to the SNS topic.
- B. Create an Amazon CloudWatch alarm for the EC2 instance, and specify the StatusCheckFailed_System metric. Add an EC2 action to the alarm to recover the instance. Add an alarm notification to publish a message to an AmazonSimple Notification Service (Amazon SNS) topic. Subscribe the SysOps team email address to the SNS topic.
- C. Create an Auto Scaling group across three different subnets in the same Availability Zone with a minimum, maximum, and desired size of 1. Configure the Auto Scaling group to use a launch template that specifies the private IP addressand the Elastic IP address. Add an activity notification for the Auto Scaling group to send an email message to the SysOps team through Amazon Simple Email Service (Amazon SES).

D. Create an Auto Scaling group across three Availability Zones with a minimum, maximum, and desired size of 1. Configure the Auto Scaling group to use a launch template that specifies the private IP address and the Elastic IP address. Add an activity notification for the Auto Scaling group to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the SysOps team email address to the SNS topic.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-cloudwatch-createalarm.html>

QUESTION 46

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 ranges. Turn on VPC Flow Logs, and send the logs to AmazonCloudWatch Logs. 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.
- B. 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 instances. If public IP addresses are found on the EC2 instances, initiate another Systems Manager Automation document to terminate the instances.
- C. Configure AWS Config and a custom rule to monitor whether a security group allows inbound requests from noncorporate CIDR ranges. Create an AWS Systems Manager Automation document to remove any noncorporate CIDR ranges from the application security groups.
- D. Configure AWS Config and the managed rule for monitoring public IP associations with the EC2 instances by tag. Tag the EC2 instances with an identifier. Create an AWS Systems Manager Automation document to remove the public IP association from the EC2 instances.

Correct Answer: A

Section: (none)

Explanation



Explanation/Reference:

QUESTION 47

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. Create an Amazon CloudFront distribution in each AWS Region, and set the S3 bucket as the origin. 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.
- B. Create an Amazon S3 bucket, and upload the website content to the S3 bucket. Create an Amazon CloudFront distribution, and set the S3 bucket as the origin. Use Amazon Route 53 to create an alias record that points to the CloudFront distribution.
- C. Create an Application Load Balancer (ALB) and a target group. Create an Amazon EC2 Auto Scaling group with at least two EC2 instances in the associated target group. Store the website content on the EC2 instances. Use Amazon Route 53 to create an alias record that points to the ALB.
- D. Create an Application Load Balancer (ALB) and a target group in two Regions. Create an Amazon EC2 Auto Scaling group in each Region with at least two EC2 instances in each target group. Store the website content on the EC2 instances. 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.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 48

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

What should a SysOps administrator do to resolve these errors?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 49

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

What is the MOST cost-effective way to resize the cluster?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 50

A SysOps administrator is deploying an application on 10 Amazon EC2 instances. The application must be highly available. The instances must be placed on distinct underlying hardware.

What should the SysOps administrator do to meet these requirements?

- A. Launch the instances into a cluster placement group in a single AWS Region.
- B. Launch the instances into a partition placement group in multiple AWS Regions.
- C. Launch the instances into a spread placement group in multiple AWS Regions.
- D. Launch the instances into a spread placement group in single AWS Region.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 51

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

Which solution will meet these requirements?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 52 A company's IT department noticed an increase in the spend of their developer AWS account. There are over 50 developers using the account, and the finance team wants to determine the service costs incurred by each developer.

What should a SysOps administrator do to collect this information? (Choose two.)

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

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 53

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

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

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



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 54 A company has multiple Amazon EC2 instances that run a resource-intensive application in a development environment. A SysOps administrator is implementing a solution to stop these EC2 instances when they are not in use.

Which solution will meet this requirement?

- A. Assess AWS CloudTrail logs to verify that there is no EC2 API activity. Invoke an AWS lambda function to stop the EC2 instances.
- B. Create an Amazon CloudWatch alarm to stop the EC2 instances when the average CPU utilization is lower than 5% for a 30-minute period.
- C. Create an Amazon CloudWatch metric to stop the EC2 instances when the VolumeReadBytes metric is lower than 500 for a 30-minute period.
- D. Use AWS Config to invoke an AWS Lambda function to stop the EC2 instances based on resource configuration changes.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference: