Question 1: **Correct**

A data analytics company uses AWS CloudFormation templates to provision their AWS infrastructure for Amazon EC2, Amazon VPC, and Amazon S3 resources. Using cross-stack referencing, a systems administrator creates a stack called `NetworkStack` which will export the `subnetId` that can be used when creating EC2 instances in another stack.

To use the exported value in another stack, which of the following functions must be used?

○ `!ImportValue` **(Correct)**

○ `!Sub`

○ `!GetAtt`

○ `!Ref`

Explanation

Correct option:

`!ImportValue`

The intrinsic function `Fn::ImportValue` returns the value of an output exported by another stack. You typically use this function to create cross-stack references.

Incorrect options:

`!Ref` - Returns the value of the specified parameter or resource.

`!GetAtt` - Returns the value of an attribute from a resource in the template.

`!Sub` - Substitutes variables in an input string with values that you specify.

Reference:

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/intrinsic-function-reference-importvalue.html

Question 2: **Correct**

An e-commerce company is running its server infrastructure on Amazon EC2 instance store-backed instances. For better performance, the company has decided to move their applications to another Amazon EC2 instance store-backed instance with a different instance type.

How will you configure a solution for this requirement?

○ **You can't resize an instance store-backed instance. Instead, you choose a new compatible instance and move your application to the new instance**

○ **Create an image of your instance, and then launch a new instance from this image with the instance type that you need. Any public IP address associated with the instance can be moved with the instance for uninterrupted access of services**

○ **Create an image of your instance, and then launch a new instance from this image with the instance type that you need. Take any Elastic IP address that you've associated with your original instance and associate it with the new instance for uninterrupted service to your application** **(Correct)**

○ **You can't resize an instance store-backed instance. Instead, configure an EBS volume to be the root device for the instance and migrate using the EBS volume**

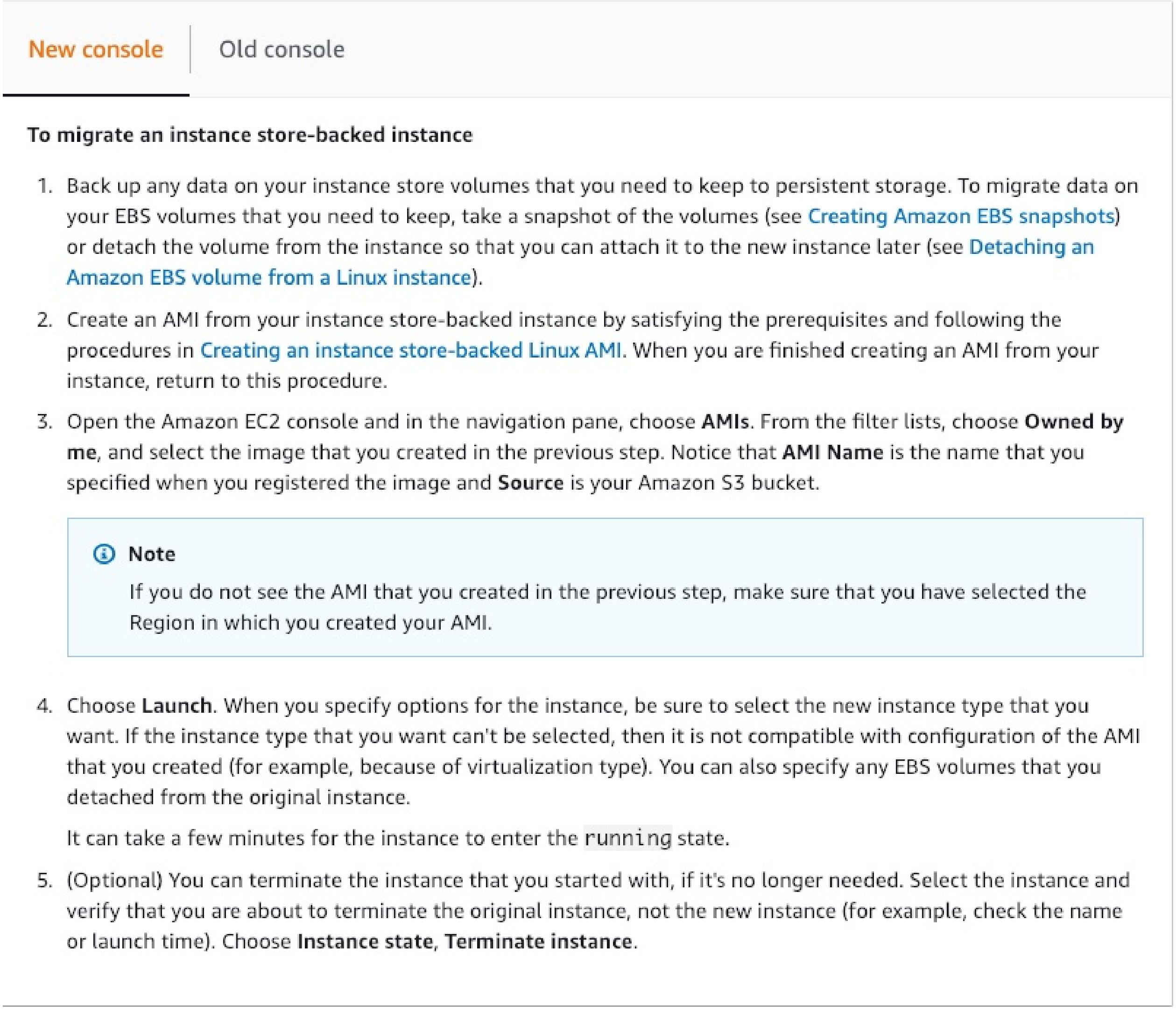
Explanation

Correct option:

Create an image of your instance, and then launch a new instance from this image with the instance type that you need. Take any Elastic IP address that you've associated with your original instance and associate it with the new instance for uninterrupted service to your application

When you want to move your application from one instance store-backed instance to an instance store-backed instance with a different instance type, you must migrate it by creating an image from your instance, and then launching a new instance from this image with the instance type that you need. To ensure that your users can continue to use the applications that you're hosting on your instance uninterrupted, you must take any Elastic IP address that you've associated with your original instance and associate it with the new instance. Then you can terminate the original instance.

Complete steps to migrate an instance store-backed instance:



To migrate an instance store-backed instance

1. Back up any data on your instance store volumes that you need to keep to persistent storage. To migrate data on your EBS volumes that you need to keep, take a snapshot of the volumes (see Creating Amazon EBS snapshots) or detach the volume from the instance so that you can attach it to the new instance later (see Detaching an Amazon EBS volume from a Linux instance).
2. Create an AMI from your instance store-backed instance by satisfying the prerequisites and following the procedures in Creating an instance store-backed Linux AMI. When you are finished creating an AMI from your instance, return to this procedure.
3. Open the Amazon EC2 console and in the navigation pane, choose **AMIs**. From the filter lists, choose **Owned by me**, and select the image that you created in the previous step. Notice that **AMI Name** is the name that you specified when you registered the image and **Source** is your Amazon S3 bucket.

   Note

   If you do not see the AMI that you created in the previous step, make sure that you have selected the Region in which you created your AMI.

4. Choose **Launch**. When you specify options for the instance, be sure to select the new instance type that you want. If the instance type that you want can't be selected, then it is not compatible with configuration of the AMI that you created (for example, because of virtualization type). You can also specify any EBS volumes that you detached from the original instance.

   It can take a few minutes for the instance to enter the `running` state.
5. (Optional) You can terminate the instance that you started with, if it's no longer needed. Select the instance and verify that you are about to terminate the original instance, not the new instance (for example, check the name or launch time). Choose **Instance state**, **Terminate instance**.

via - https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-resize.html

Incorrect options:

You can't resize an instance store-backed instance. Instead, you choose a new compatible instance and move your application to the new instance - An instance store-backed EC2 instance can be resized, as explained above.

You can't resize an instance store-backed instance. Instead, configure an EBS volume to be the root device for the instance and migrate using the EBS volume - This statement is incorrect.

Create an image of your instance, and then launch a new instance from this image with the instance type that you need. Any public IP address associated with the instance can be moved with the instance for uninterrupted access of services - Public IP addresses are released when an instance is changed. You need an Elastic IP to keep the service uninterrupted for users since these can be moved across instances.

Reference:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-resize.html

Question 3: **Correct**

A systems administrator has attached two policies to an IAM user. The first policy states that the user has explicitly been denied all access to EC2 instances. The second policy states that the user has been allowed permission for EC2:Describe action.

When the user tries to use 'Describe' action on an EC2 instance using the CLI, what will be the output?

○ **The user will get access because it has an explicit allow**

○ **The user will be denied access because one of the policies has an explicit deny on it** **(Correct)**

○ **The IAM user stands in an invalid state, because of conflicting policies**

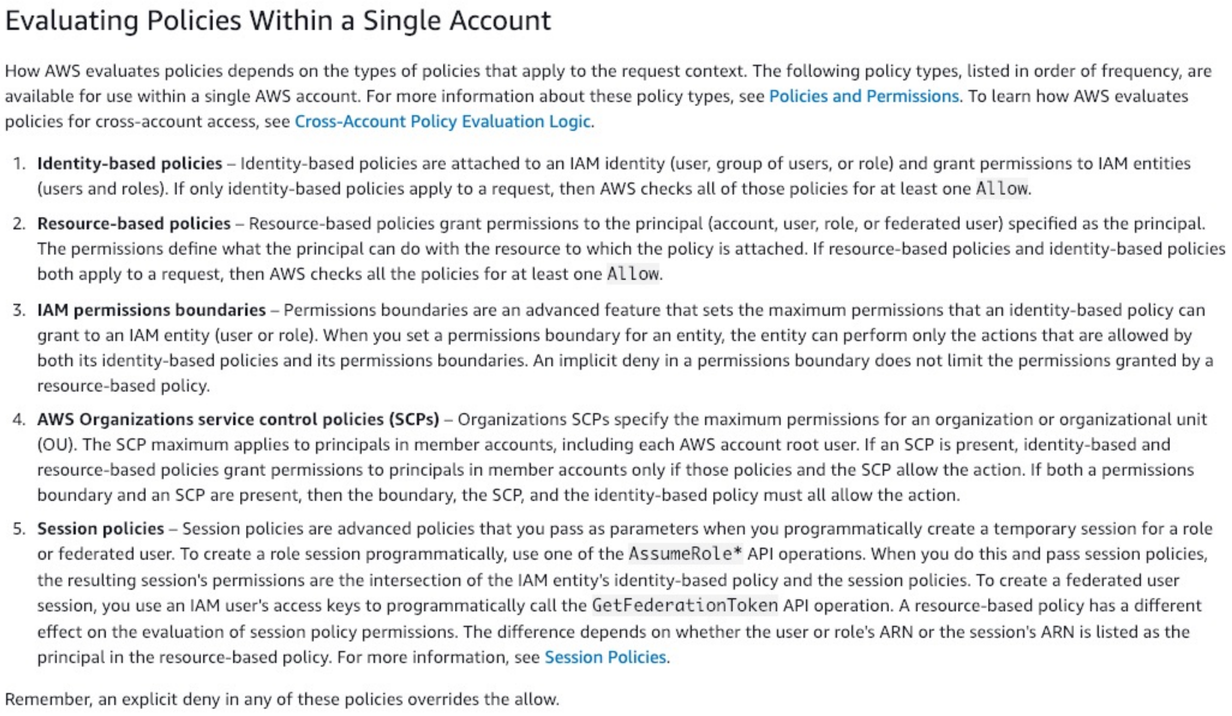
○ **The order of the policy matters. If policy 1 is before 2, then the user is denied access. If policy 2 is before 1, then the user is allowed access**

Explanation

Correct option:

The user will be denied access because the policy has an explicit deny on it - User will be denied access because any explicit deny overrides the allow.

Policy Evaluation explained:



Evaluating Policies Within a Single Account

How AWS evaluates policies depends on the types of policies that apply to the request context. The following policy types, listed in order of frequency, are available for use within a single AWS account. For more information about these policy types, see Policies and Permissions. To learn how AWS evaluates policies for cross-account access, see Cross-Account Policy Evaluation Logic.

1. **Identity-based policies** – Identity-based policies are attached to an IAM identity (user, group of users, or role) and grant permissions to IAM entities (users and roles). If only identity-based policies apply to a request, then AWS checks all of those policies for at least one `Allow`.
2. **Resource-based policies** – Resource-based policies grant permissions to the principal (account, user, role, or federated user) specified as the principal. The permissions define what the principal can do with the resource to which the policy is attached. If resource-based policies and identity-based policies both apply to a request, then AWS checks all the policies for at least one `Allow`.
3. **IAM permissions boundaries** – Permissions boundaries are an advanced feature that sets the maximum permissions that an identity-based policy can grant to an IAM entity (user or role). When you set a permissions boundary for an entity, the entity can perform only the actions that are allowed by both its identity-based policies and its permissions boundaries. An implicit deny in a permissions boundary does not limit the permissions granted by a resource-based policy.
4. **AWS Organizations service control policies (SCPs)** – Organizations SCPs specify the maximum permissions for an organization or organizational unit (OU). The SCP maximum applies to principals in member accounts, including each AWS account root user. If an SCP is present, identity-based and resource-based policies grant permissions to principals in member accounts only if those policies and the SCP allow the action. If both a permissions boundary and an SCP are present, then the boundary, the SCP, and the identity-based policy must all allow the action.
5. **Session policies** – Session policies are advanced policies that you pass as parameters when you programmatically create a temporary session for a role or federated user. To create a role session programmatically, use one of the `AssumeRole*` API operations. When you do this and pass session policies, the resulting session's permissions are the intersection of the IAM entity's identity-based policy and the session policies. To create a federated user session, you use an IAM user's access keys to programmatically call the `GetFederationToken` API operation. A resource-based policy has a different effect on the evaluation of session policy permissions. The difference depends on whether the user or role's ARN or the session's ARN is listed as the principal in the resource-based policy. For more information, see Session Policies.

Remember, an explicit deny in any of these policies overrides the allow.

via - https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html

Incorrect options:

The IAM user stands in an invalid state, because of conflicting policies - This is an incorrect statement. Access policies can have allow and deny permissions on them and based on policy rules they are evaluated. A user account does not get invalid because of policies.

The user will get access because it has an explicit allow - As discussed above, explicit deny overrides all other permissions and hence the user will be denied access.

The order of the policy matters. If policy 1 is before 2, then the user is denied access. If policy 2 is before 1, then the user is allowed access - If policies that apply to a request include an Allow statement and a Deny statement, the Deny statement trumps the Allow statement. The request is explicitly denied.

Reference:

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html

Question 4: **Skipped**

An analytics company generates reports for various client applications, some of which have critical data. As per the company's compliance guidelines, data has to be encrypted during data exchange, for all channels of communication. An Amazon S3 bucket is configured as a website endpoint and this is now being added as a custom origin for CloudFront.

How will you secure this channel, as per the company's requirements?

○ **Communication between CloudFront and Amazon S3 is always on HTTP protocol since the network used for communication is internal to AWS and is inherently secure**

○ **Configure CloudFront to mandate viewers to use HTTPS to request objects from S3. However, CloudFront and S3 will use HTTP to communicate with each other** **(Correct)**

○ **CloudFront always forwards requests to S3 by using the protocol that viewers used to submit the requests. So, we only need to configure CloudFront to mandate the use of HTTPS for users**

○ **Configure CloudFront that mandates viewers to use HTTPS to request objects from S3. Configure S3 bucket to support HTTPS communication only. This will force CloudFront to use HTTPS for communication between CloudFront and S3**

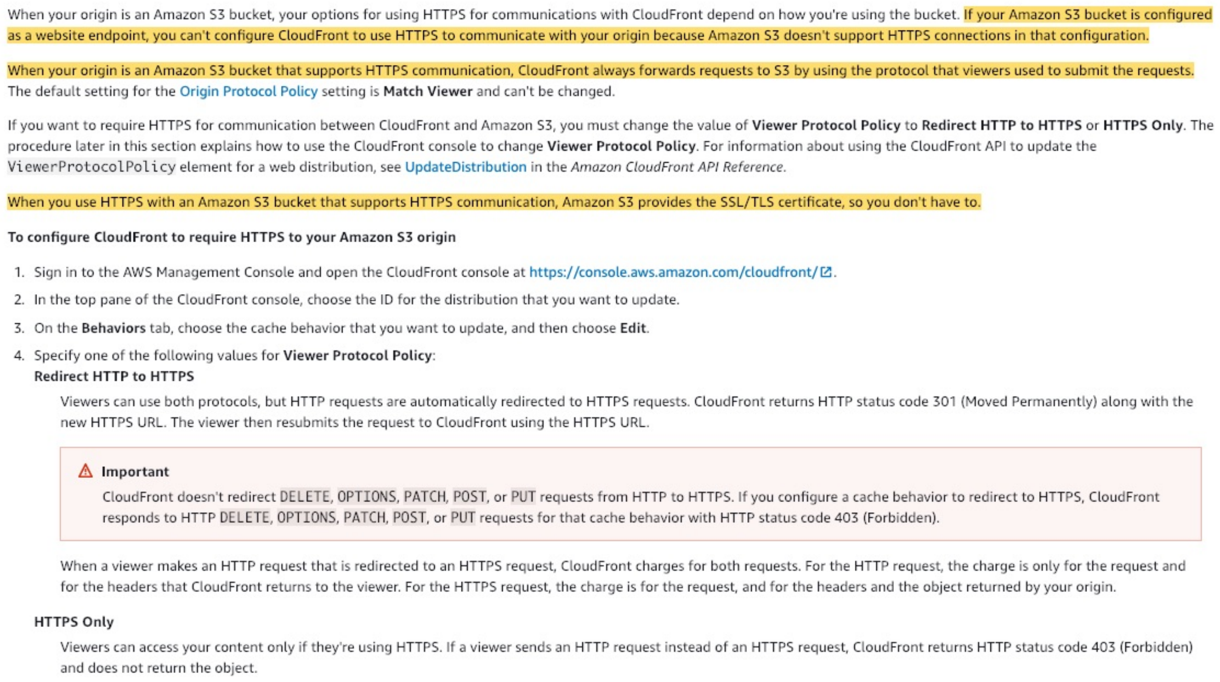
Explanation

Correct option:

Configure CloudFront to mandate viewers to use HTTPS to request objects from S3. CloudFront and S3 will use HTTP to communicate with each other

If your Amazon S3 bucket is configured as a website endpoint, you can't configure CloudFront to use HTTPS to communicate with your origin because Amazon S3 doesn't support HTTPS connections in that configuration.

HTTPS for Communication Between CloudFront and Your Amazon S3 Origin:



When your origin is an Amazon S3 bucket, your options for using HTTPS for communications with CloudFront depend on how you're using the bucket. If your Amazon S3 bucket is configured as a website endpoint, you can't configure CloudFront to use HTTPS to communicate with your origin because Amazon S3 doesn't support HTTPS connections in that configuration.

When your origin is an Amazon S3 bucket that supports HTTPS communication, CloudFront always forwards requests to S3 by using the protocol that viewers used to submit the requests. The default setting for the Origin Protocol Policy setting is **Match Viewer** and can't be changed.

If you want to require HTTPS for communication between CloudFront and Amazon S3, you must change the value of **Viewer Protocol Policy** to **Redirect HTTP to HTTPS** or **HTTPS Only**. The procedure later in this section explains how to use the CloudFront console to change **Viewer Protocol Policy**. For information about using the CloudFront API to update the `ViewerProtocolPolicy` element for a web distribution, see UpdateDistribution in the *Amazon CloudFront API Reference*.

When you use HTTPS with an Amazon S3 bucket that supports HTTPS communication, Amazon S3 provides the SSL/TLS certificate, so you don't have to.

To configure CloudFront to require HTTPS to your Amazon S3 origin

1. Sign in to the AWS Management Console and open the CloudFront console at https://console.aws.amazon.com/cloudfront/.
2. In the top pane of the CloudFront console, choose the ID for the distribution that you want to update.
3. On the **Behaviors** tab, choose the cache behavior that you want to update, and then choose **Edit**.
4. Specify one of the following values for **Viewer Protocol Policy**:

Redirect HTTP to HTTPS

Viewers can use both protocols, but HTTP requests are automatically redirected to HTTPS requests. CloudFront returns HTTP status code 301 (Moved Permanently) along with the new HTTPS URL. The viewer then resubmits the request to CloudFront using the HTTPS URL.

> ⚠ **Important**
>
> CloudFront doesn't redirect `DELETE`, `OPTIONS`, `PATCH`, `POST`, or `PUT` requests from HTTP to HTTPS. If you configure a cache behavior to redirect to HTTPS, CloudFront responds to HTTP `DELETE`, `OPTIONS`, `PATCH`, `POST`, or `PUT` requests for that cache behavior with HTTP status code 403 (Forbidden).

When a viewer makes an HTTP request that is redirected to an HTTPS request, CloudFront charges for both requests. For the HTTP request, the charge is only for the request and for the headers that CloudFront returns to the viewer. For the HTTPS request, the charge is for the request, and for the headers and the object returned by your origin.

HTTPS Only

Viewers can access your content only if they're using HTTPS. If a viewer sends an HTTP request instead of an HTTPS request, CloudFront returns HTTP status code 403 (Forbidden) and does not return the object.

via - https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-cloudfront-to-s3-origin.html

Incorrect options:

Configure CloudFront that mandates viewers to use HTTPS to request objects from S3. Configure S3 bucket to support HTTPS communication only. This will force CloudFront to use HTTPS for communication between CloudFront and S3 - As discussed above, HTTPS between CloudFront and Amazon S3 is not supported when the S3 bucket is configured as a website endpoint.

Communication between CloudFront and Amazon S3 is always on HTTP protocol since the network used for communication is internal to AWS and is inherently secure - When your origin is an Amazon S3 bucket, your options for using HTTPS for communications with CloudFront depend on how you're using the bucket. If your Amazon S3 bucket is configured as a website endpoint, you can't configure CloudFront to use HTTPS to communicate with your origin.

When your origin is an Amazon S3 bucket that supports HTTPS communication, CloudFront always forwards requests to S3 by using the protocol that viewers used to submit the requests.

CloudFront always forwards requests to S3 by using the protocol that viewers used to submit the requests. So, we only need to configure CloudFront to mandate the use of HTTPS for users - This option has been added as a distractor. As mentioned earlier, if your Amazon S3 bucket is configured as a website endpoint, you can't configure CloudFront to use HTTPS while communicating with S3.

Reference:

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-cloudfront-to-s3-origin.html

Question 5: **Correct**

As part of the systems administration work, an AWS Certified SysOps Administrator is creating policies and attaching them to IAM identities. After creating necessary Identity-based policies, he is now creating Resource-based policies.

Which is the only resource-based policy that the IAM service supports?

○ **Access control list (ACL)**

○ **AWS Organizations Service Control Policies (SCP)**

○ **Trust policy** **(Correct)**

○ **Permissions boundary**

Explanation

Correct option:

You manage access in AWS by creating policies and attaching them to IAM identities (users, groups of users, or roles) or AWS resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. Resource-based policies are JSON policy documents that you attach to a resource such as an Amazon S3 bucket. These policies grant the specified principal permission to perform specific actions on that resource and define under what conditions this applies.

Trust policy - Trust policies define which principal entities (accounts, users, roles, and federated users) can assume the role. An IAM role is both an identity and a resource that supports resource-based policies. For this reason, you must attach both a trust policy and an identity-based policy to an IAM role. The IAM service supports only one type of resource-based policy called a role trust policy, which is attached to an IAM role.

Incorrect options:

AWS Organizations Service Control Policies (SCP) - If you enable all features of AWS organization, then you can apply service control policies (SCPs) to any or all of your accounts. SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU). The SCP limits permissions for entities in member accounts, including each AWS account root user. An explicit deny in any of these policies overrides the allow.

Access control list (ACL) - Access control lists (ACLs) are service policies that allow you to control which principals in another account can access a resource. ACLs cannot be used to control access for a principal within the same account. Amazon S3, AWS WAF, and Amazon VPC are examples of services that support ACLs.

Permissions boundary - AWS supports permissions boundaries for IAM entities (users or roles). A permissions boundary is an advanced feature for using a managed policy to set the maximum permissions that an identity-based policy can grant to an IAM entity. An entity's permissions boundary allows it to perform only the actions that are allowed by both its identity-based policies and its permissions boundaries.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html#policies_resource-based

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html

Question 6: **Correct**

A systems administration intern is trying to configure what an Amazon EC2 should do when it interrupts a Spot Instance.

Which of the following CANNOT be configured as an interruption behavior?

○ **Stop the Spot Instance**

○ **Reboot the Spot Instance** **(Correct)**

○ **Hibernate the Spot Instance**

○ **Terminate the Spot Instance**

Explanation

Correct option:

A Spot Instance is an unused EC2 instance that is available for less than the On-Demand price. Your Spot Instance runs whenever capacity is available and the maximum price per hour for your request exceeds the Spot price. Any instance present with unused capacity will be allocated.

You can specify that Amazon EC2 should do one of the following when it interrupts a Spot Instance:

Stop the Spot Instance

Hibernate the Spot Instance

Terminate the Spot Instance

The default is to terminate Spot Instances when they are interrupted.

Reboot the Spot Instance - This is an invalid option.

Incorrect options:

It is always possible that Spot Instances might be interrupted. Therefore, you must ensure that your application is prepared for a Spot Instance interruption.

Stop the Spot Instance - This is a valid option. Amazon EC2 can be configured to stop the instance when an interruption occurs on Spot instances.

Hibernate the Spot Instance - This is a valid option. Amazon EC2 can be configured to hibernate the instance when an interruption occurs on Spot instances.

Terminate the Spot Instance - This is a valid option. Amazon EC2 can be configured to hibernate the instance when an interruption occurs on Spot instances. The default behavior is to terminate Spot Instances when they are interrupted.

Reference:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/spot-interruptions.html

Question 7: **Correct**

A company uses Amazon S3 bucket replication to copy data from one S3 bucket into the other, for compliance purposes. The Technical Lead of the development team wants to be notified if replication of an object across S3 buckets fails.

How will you configure this automatic notification?

○ **Use Amazon Simple Queue Service (Amazon SQS) queue to copy objects from one S3 bucket to the other. If replication fails, messages in the queue can be configured to send notification using SNS**

○ **Amazon S3 publishes object events to CloudWatch. Configure Amazon Simple Notification Service (Amazon SNS) to send notifications for replication failure of objects**

○ **Enable S3 Replication with Notification, which allows you to set up notifications for objects that failed replication**

○ **Enable S3 Replication Time Control (S3 RTC), which allows you to set up notifications for eligible objects that failed replication** **(Correct)**

Explanation

Correct option:

Enable S3 Replication Time Control (S3 RTC), which allows you to set up notifications for eligible objects that failed replication

S3 Replication Time Control (S3 RTC) helps you meet compliance or business requirements for data replication and provides visibility into Amazon S3 replication times. S3 RTC replicates most objects that you upload to Amazon S3 in seconds, and 99.99 percent of those objects within 15 minutes.

S3 RTC by default includes S3 replication metrics and S3 event notifications, with which you can monitor the total number of S3 API operations that are pending replication, the total size of objects pending replication, and the maximum replication time.

You can track replication time for objects that did not replicate within 15 minutes by monitoring specific event notifications that S3 Replication Time Control (S3 RTC) publishes. These events are published when an object that was eligible for replication using S3 RTC didn't replicate within 15 minutes, and when that object replicates to the destination Region.

Replication events are available within 15 minutes of enabling S3 RTC. Amazon S3 events are available through Amazon SQS, Amazon SNS, or AWS Lambda.

Incorrect options:

Enable S3 Replication with Notification, which allows you to set up notifications for objects that failed replication - This is a made-up option and given only as a distractor.

Use Amazon Simple Queue Service (Amazon SQS) queue to copy objects from one S3 bucket to the other. If replication fails, messages in the queue can be configured to send notifications using SNS - Amazon S3 offers a direct replication feature. Hence, a custom logic to do the same does not make sense.

Amazon S3 publishes object events to CloudWatch. Configure Amazon Simple Notification Service (Amazon SNS) to send notifications for replication failure of objects - Amazon S3 replication events are only published if you have enabled S3 Replication Time Control, for replication.

Reference:

https://docs.aws.amazon.com/AmazonS3/latest/dev/replication-time-control.html#using-s3-events-to-track-rtc

Question 8: **Incorrect**

A video streaming solutions company wants to use AWS Cloudfront to distribute its content only to its service subscribers.

As a SysOps Administrator, which of the following solutions would you suggest in order to deliver restricted content to the subscribers? (Select two)

□ Use CloudFront signed cookies (Correct)

□ Forward HTTPS requests to the origin server by using the ECDSA or RSA ciphers

□ Require HTTPS for communication between CloudFront and your S3 origin

□ Use CloudFront signed URLs (Correct)

Require HTTPS for communication between CloudFront and your custom origin (Incorrect)

Explanation

Correct options:

Use CloudFront signed URLs

Many companies that distribute content over the internet want to restrict access to documents, business data, media streams, or content that is intended for selected users, for example, users who have paid a fee.

To securely serve this private content by using CloudFront, you can do the following:

Require that your users access your private content by using special CloudFront signed URLs or signed cookies.

A signed URL includes additional information, for example, expiration date and time, that gives you more control over access to your content. So this is the correct option.

Use CloudFront signed cookies

CloudFront signed cookies allow you to control who can access your content when you don't want to change your current URLs or when you want to provide access to multiple restricted files, for example, all of the files in the subscribers' area of a website. So this is also a correct option.

Incorrect options:

Require HTTPS for communication between CloudFront and your custom origin

Require HTTPS for communication between CloudFront and your S3 origin

Requiring HTTPS for communication between CloudFront and your custom origin (or S3 origin) only enables secure access to the underlying content. You cannot use HTTPS to restrict access to your private content. So both these options are incorrect.

Forward HTTPS requests to the origin server by using the ECDSA or RSA ciphers - This option is just added as a distractor. You cannot use HTTPS to restrict access to your private content.

References:

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-cookies.html

Question 9: **Incorrect**

A multi-national retail company uses AWS Organizations to manage its users across different divisions. Even though CloudTrail is enabled on the member AWS accounts, managers have noticed that access issues for CloudTrail logs across different divisions and AWS Regions are becoming a bottleneck in troubleshooting issues. They have decided to use the organization trail to keep things simple.

What are the important points to remember when configuring an organization trail? (Select two)

There is nothing called Organization Trail. The master account can, however, enable CloudTrail logging, to keep track of all activities across AWS accounts

Member accounts do not have access to organization trail, neither do they have access to the Amazon S3 bucket that logs the files

By default, CloudTrail event log files are not encrypted	(Incorrect)
By default, CloudTrail tracks only bucket-level actions. To track object-level actions, you need to enable Amazon S3 data events	(Correct)
Member accounts will be able to see the Organization trail, but cannot modify or delete it	(Correct)

Explanation

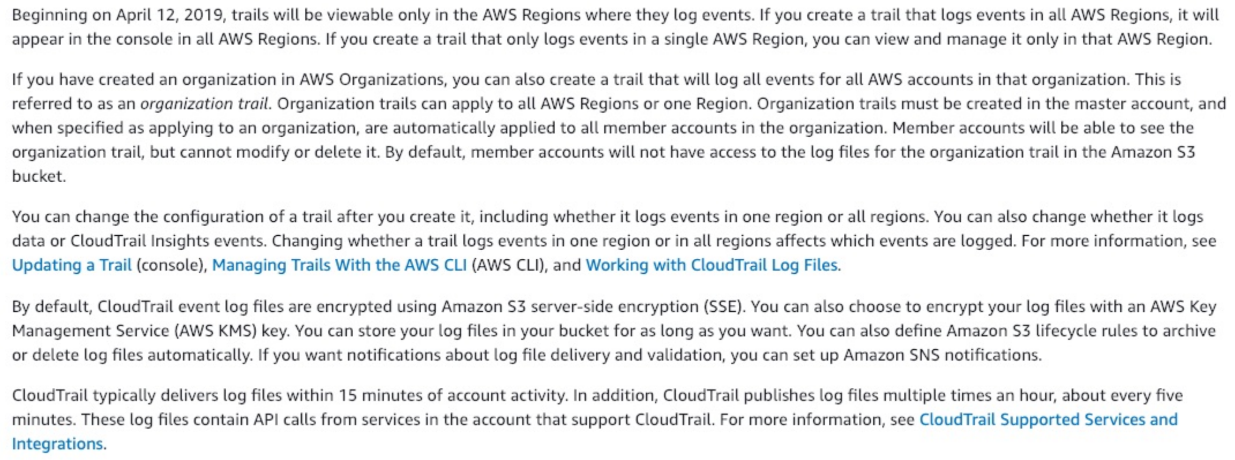
Correct option:

If you have created an organization in AWS Organizations, you can also create a trail that will log all events for all AWS accounts in that organization. This is referred to as an organization trail.

By default, CloudTrail tracks only bucket-level actions. To track object-level actions, you need to enable Amazon S3 data events - This is a correct statement. AWS CloudTrail supports Amazon S3 Data Events, apart from bucket Events. You can record all API actions on S3 Objects and receive detailed information such as the AWS account of the caller, IAM user role of the caller, time of the API call, IP address of the API, and other details. All events are delivered to an S3 bucket and CloudWatch Events, allowing you to take programmatic actions on the events.

Member accounts will be able to see the organization trail, but cannot modify or delete it - Organization trails must be created in the master account, and when specified as applying to an organization, are automatically applied to all member accounts in the organization. Member accounts will be able to see the organization trail, but cannot modify or delete it. By default, member accounts will not have access to the log files for the organization trail in the Amazon S3 bucket.

Organization trail:



Beginning on April 12, 2019, trails will be viewable only in the AWS Regions where they log events. If you create a trail that logs events in all AWS Regions, it will appear in the console in all AWS Regions. If you create a trail that only logs events in a single AWS Region, you can view and manage it only in that AWS Region.

If you have created an organization in AWS Organizations, you can also create a trail that will log all events for all AWS accounts in that organization. This is referred to as an *organization trail*. Organization trails can apply to all AWS Regions or one Region. Organization trails must be created in the master account, and when specified as applying to an organization, are automatically applied to all member accounts in the organization. Member accounts will be able to see the organization trail, but cannot modify or delete it. By default, member accounts will not have access to the log files for the organization trail in the Amazon S3 bucket.

You can change the configuration of a trail after you create it, including whether it logs events in one region or all regions. You can also change whether it logs data or CloudTrail Insights events. Changing whether a trail logs events in one region or in all regions affects which events are logged. For more information, see Updating a Trail (console), Managing Trails With the AWS CLI (AWS CLI), and Working with CloudTrail Log Files.

By default, CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE). You can also choose to encrypt your log files with an AWS Key Management Service (AWS KMS) key. You can store your log files in your bucket for as long as you want. You can also define Amazon S3 lifecycle rules to archive or delete log files automatically. If you want notifications about log file delivery and validation, you can set up Amazon SNS notifications.

CloudTrail typically delivers log files within 15 minutes of account activity. In addition, CloudTrail publishes log files multiple times an hour, about every five minutes. These log files contain API calls from services in the account that support CloudTrail. For more information, see CloudTrail Supported Services and Integrations.

via - https://docs.aws.amazon.com/awscloudtrail/latest/userguide/how-cloudtrail-works.html

Incorrect options:

There is nothing called Organization Trail. The master account can, however, enable CloudTrail logging, to keep track of all activities across AWS accounts - This statement is incorrect. AWS offers Organization Trail for easy management and monitoring.

Member accounts do not have access to the organization trail, neither do they have access to the Amazon S3 bucket that logs the files - This statement is only partially correct. Member accounts will be able to see the organization trail, but cannot modify or delete it. By default, member accounts will not have access to the log files for the organization trail in the Amazon S3 bucket.

By default, CloudTrail event log files are not encrypted - This is an incorrect statement. By default, CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE).

References:

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/how-cloudtrail-works.html

https://aws.amazon.com/about-aws/whats-new/2016/11/aws-cloudtrail-supports-s3-data-events/

https://aws.amazon.com/premiumsupport/knowledge-center/secure-s3-resources/

Question 10: **Correct**

A social media company is using AWS CloudFormation to manage its technology infrastructure. It has created a template to provision a stack with a VPC and a subnet. The output value of this subnet has to be used in another stack.

As a SysOps Administrator, which of the following options would you suggest to provide this information to the other stack?

○ **Use Fn::ImportValue**

○ **Use 'Expose' field in the Output section of the stack's template**

○ **Use 'Export' field in the Output section of the stack's template** **(Correct)**

○ **Use Fn::Transform**

Explanation

Correct option:

Use 'Export' field in the Output section of the stack's template

To share information between stacks, export a stack's output values. Other stacks that are in the same AWS account and region can import the exported values.

To export a stack's output value, use the Export field in the Output section of the stack's template. To import those values, use the Fn::ImportValue function in the template for the other stacks.

Incorrect options:

Use 'Expose' field in the Output section of the stack's template - 'Expose' is a made-up option, and only given as a distractor.

Use Fn::ImportValue - To import the values exported by another stack, we use the Fn::ImportValue function in the template for the other stacks. This function is not useful for the current scenario.

Use Fn::Transform - The intrinsic function Fn::Transform specifies a macro to perform custom processing on part of a stack template. Macros enable you to perform custom processing on templates, from simple actions like find-and-replace operations to extensive transformations of entire templates. This function is not useful for the current scenario.

Reference:

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-stack-exports.html

Question 11: **Correct**

A data analytics company runs its technology operations on AWS Cloud using different VPC configurations for each of its applications. A systems administrator wants to configure the Network Access Control List (ACL) and Security Group (SG) of VPC1 to allow access for AWS resources in VPC2.

Which is the best way of configuring this requirement?

○ **Based on the inbound and outbound traffic configurations on Network ACL of VPC1, you can create a similar deny rules on Security Groups of the instances in VPC1 to deny all traffic, other than the one originating from resources in VPC2**

○ The Security Groups of instances on VPC1 should be configured to allow inbound traffic from resources in VPC2. By default, Network ACLs allow all inbound and outbound traffic. So, a default Network ACLs on VPC1 will not need any configuration changes (Correct)

○ By default, Security Groups allow outbound traffic. Hence, only the inbound traffic configuration of the security groups have to be changed to allow requests from resources in VPC2 to access instances in VPC1. If the subnet is not associated with any Network ACL, you will not need any configuration changes

○ Network ACLs and Security Groups share a parent-child relationship. If resources in VPC2 are given inbound and outbound permissions on Network ACLs of VPC1, the resources will get necessary permissions on the associated security groups too

Explanation

Correct option:

The Security Groups of instances on VPC1 should be configured to allow inbound traffic from resources in VPC2. By default, Network ACLs allow all inbound and outbound traffic. So, a default Network ACLs on VPC1 will not need any configuration changes - A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC can be assigned to a different set of security groups.

A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

Security groups are stateful — if you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules. Responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules.

Network ACLs are stateless, which means that responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa).

Incorrect options:

Network ACLs and Security Groups share a parent-child relationship. If resources in VPC2 are given inbound and outbound permissions on Network ACLs of VPC1, the resources will get necessary permissions on the associated security groups too - This is an incorrect statement. Security Groups act at the instance level and Network ACLs are at the subnet level. They are different levels of security provided by AWS and do not form any hierarchy.

By default, Security Groups allow outbound traffic. Hence, only the inbound traffic configuration of the security groups have to be changed to allow requests from resources in VPC2 to access instances in VPC1. If the subnet is not associated with any Network ACL, you will not need any configuration changes - Each subnet in your VPC must be associated with a network ACL. If you don't explicitly associate a subnet with a network ACL, the subnet is automatically associated with the default network ACL. Hence, a subnet will always have a network ACL associated with it.

Based on the inbound and outbound traffic configurations on Network ACL of VPC1, you can create similar deny rules on Security Groups of the instances in VPC1 to deny all traffic, other than the one originating from resources in VPC2 - Security Groups and Network ACLs are mutually exclusive and do not share permissions. Also, Security Groups can only be used to specify allow rules, and not deny rules.

References:

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

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

Question 12: **Incorrect**

A Systems Administrator is configuring an Application Load Balancer (ALB) that fronts Amazon EC2 instances.

Which of the following options would you identify as correct for configuring the ALB? (Select two)

□ **The targets of a target group in an ALB should all belong to the same Availability Zone**

□ **You configure target groups of an ALB by attaching them to the listeners** **(Correct)**

□ **A target can be registered with only one target group at any given time**

When you create a listener, you define actions and conditions for the default rule (Incorrect)

Before you start using your Application Load Balancer, you must add one or more listeners (Correct)

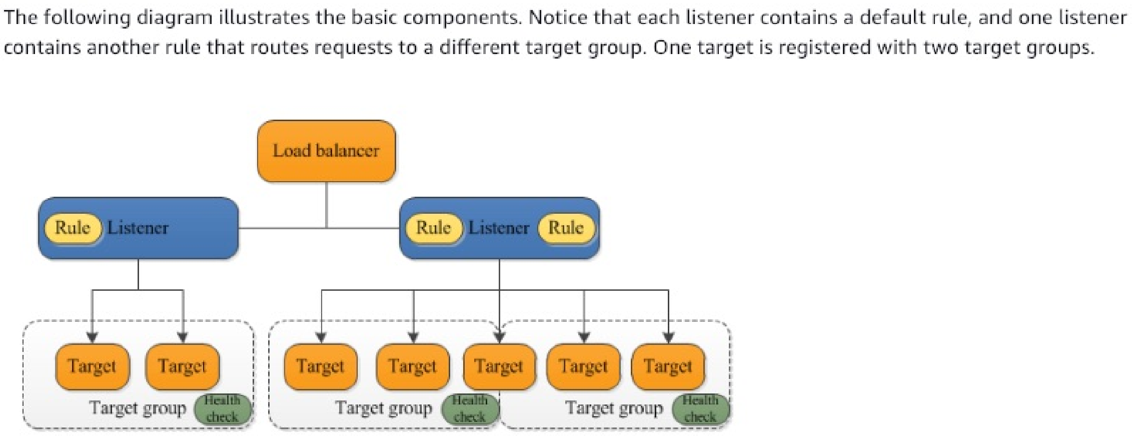
Explanation

Correct options:

Before you start using your Application Load Balancer, you must add one or more listeners - A listener checks for connection requests from clients, using the protocol and port that you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets. Each rule consists of a priority, one or more actions, and one or more conditions. When the conditions for a rule are met, then its actions are performed. You must define a default rule for each listener, and you can optionally define additional rules.

You configure target groups of an ALB by attaching them to the listeners - Each target group is used to route requests to one or more registered targets. When you create each listener rule, you specify a target group and conditions. When a rule condition is met, traffic is forwarded to the corresponding target group. You can create different target groups for different types of requests.

Load Balancer basic components:



The following diagram illustrates the basic components. Notice that each listener contains a default rule, and one listener contains another rule that routes requests to a different target group. One target is registered with two target groups.

via - https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html

Incorrect options:

The targets of a target group in an ALB should all belong to the same Availability Zone - A load balancer serves as the single point of contact for clients. The load balancer distributes incoming application traffic across multiple targets, such as EC2 instances, in multiple Availability Zones. This increases the availability of your application.

A target can be registered with only one target group at any given time - Each target group routes requests to one or more registered targets, such as EC2 instances, using the protocol and port number that you specify. You can register a target with multiple target groups.

When you create a listener, you define actions and conditions for the default rule - When you create a listener, you define actions for the default rule. Default rules can't have conditions. If the conditions for none of a listener's rules are met, then the action for the default rule is performed.

Reference:

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-listeners.html

Question 13: **Correct**

A financial services startup is building an interactive tool for personal finance needs. The users would be required to capture their financial data via this tool. As this is sensitive information, the backup of the user data must be kept encrypted in S3. The startup does not want to provide its own encryption keys but still wants to maintain an audit trail of when an encryption key was used and by whom.

Which of the following is the BEST solution for this use-case?

○ **Use SSE-KMS to encrypt the user data on S3** **(Correct)**

○ **Use SSE-S3 to encrypt the user data on S3**

○ **Use SSE-C to encrypt the user data on S3**

○ **Use client-side encryption with client provided keys and then upload the encrypted user data to S3**

Explanation

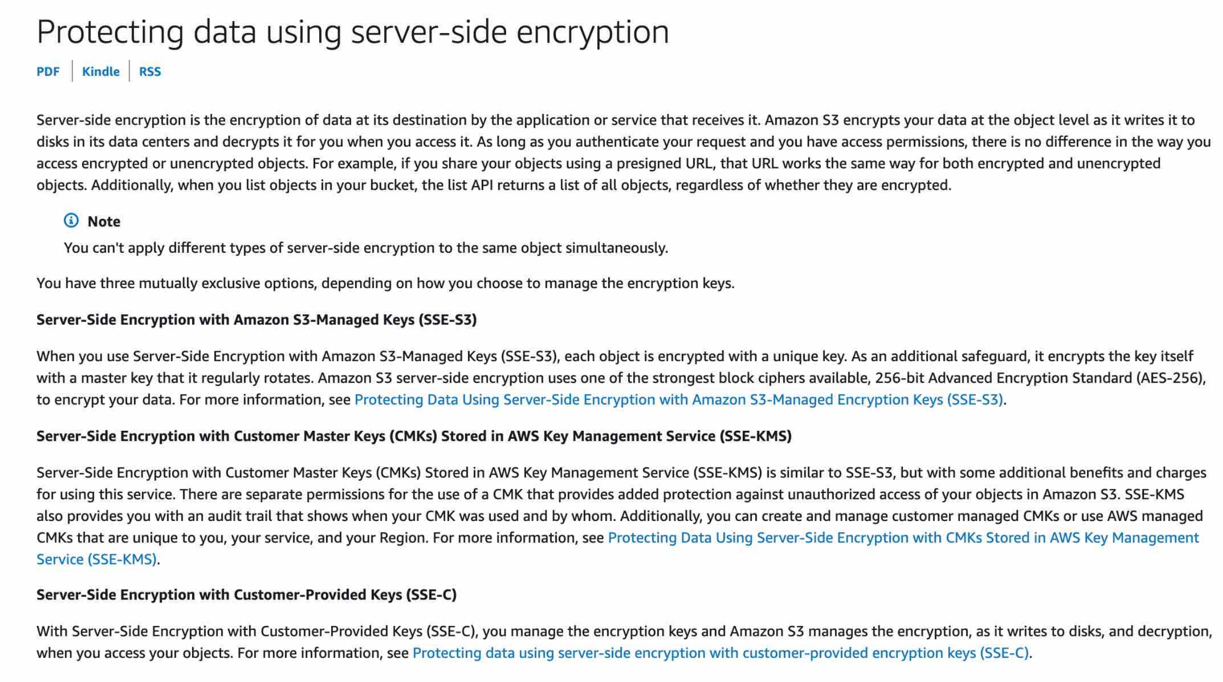
Correct option:

Use SSE-KMS to encrypt the user data on S3

AWS Key Management Service (AWS KMS) is a service that combines secure, highly available hardware and software to provide a key management system scaled for the cloud. When you use server-side encryption with AWS KMS (SSE-KMS), you can specify a customer-managed CMK that you have already created.

SSE-KMS provides you with an audit trail that shows when your CMK was used and by whom. Therefore SSE-KMS is the correct solution for this use-case.

Server Side Encryption in S3:



Protecting data using server-side encryption

PDF | Kindle | RSS

Server-side encryption is the encryption of data at its destination by the application or service that receives it. Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. As long as you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects. For example, if you share your objects using a presigned URL, that URL works the same way for both encrypted and unencrypted objects. Additionally, when you list objects in your bucket, the list API returns a list of all objects, regardless of whether they are encrypted.

> **Note**
>
> You can't apply different types of server-side encryption to the same object simultaneously.

You have three mutually exclusive options, depending on how you choose to manage the encryption keys.

Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

When you use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3), each object is encrypted with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data. For more information, see Protecting Data Using Server-Side Encryption with Amazon S3-Managed Encryption Keys (SSE-S3).

Server-Side Encryption with Customer Master Keys (CMKs) Stored in AWS Key Management Service (SSE-KMS)

Server-Side Encryption with Customer Master Keys (CMKs) Stored in AWS Key Management Service (SSE-KMS) is similar to SSE-S3, but with some additional benefits and charges for using this service. There are separate permissions for the use of a CMK that provides added protection against unauthorized access of your objects in Amazon S3. SSE-KMS also provides you with an audit trail that shows when your CMK was used and by whom. Additionally, you can create and manage customer managed CMKs or use AWS managed CMKs that are unique to you, your service, and your Region. For more information, see Protecting Data Using Server-Side Encryption with CMKs Stored in AWS Key Management Service (SSE-KMS).

Server-Side Encryption with Customer-Provided Keys (SSE-C)

With Server-Side Encryption with Customer-Provided Keys (SSE-C), you manage the encryption keys and Amazon S3 manages the encryption, as it writes to disks, and decryption, when you access your objects. For more information, see Protecting data using server-side encryption with customer-provided encryption keys (SSE-C).

via - https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html

Incorrect options:

Use SSE-S3 to encrypt the user data on S3 - When you use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3), each object is encrypted with a unique key. However, this option does not provide the ability to audit trail the usage of the encryption keys.

Use SSE-C to encrypt the user data on S3 - With Server-Side Encryption with Customer-Provided Keys (SSE-C), you manage the encryption keys and Amazon S3 manages the encryption, as it writes to disks, and decryption when you access your objects. However, this option does not provide the ability to audit trail the usage of the encryption keys.

Use client-side encryption with client provided keys and then upload the encrypted user data to S3 - Using client-side encryption is ruled out as the startup does not want to provide the encryption keys.

References:

https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html

https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html

https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html

Question 14: **Correct**

Your application is hosted by a provider on yourapp.freehosting.com. You would like to have your users access your application using www.yourdomain.com, which you own and manage under Route 53.

What Route 53 record should you create?

○ Create an A record

○ Create a PTR record

○ Create a CNAME record (Correct)

○ Create an Alias Record

Explanation

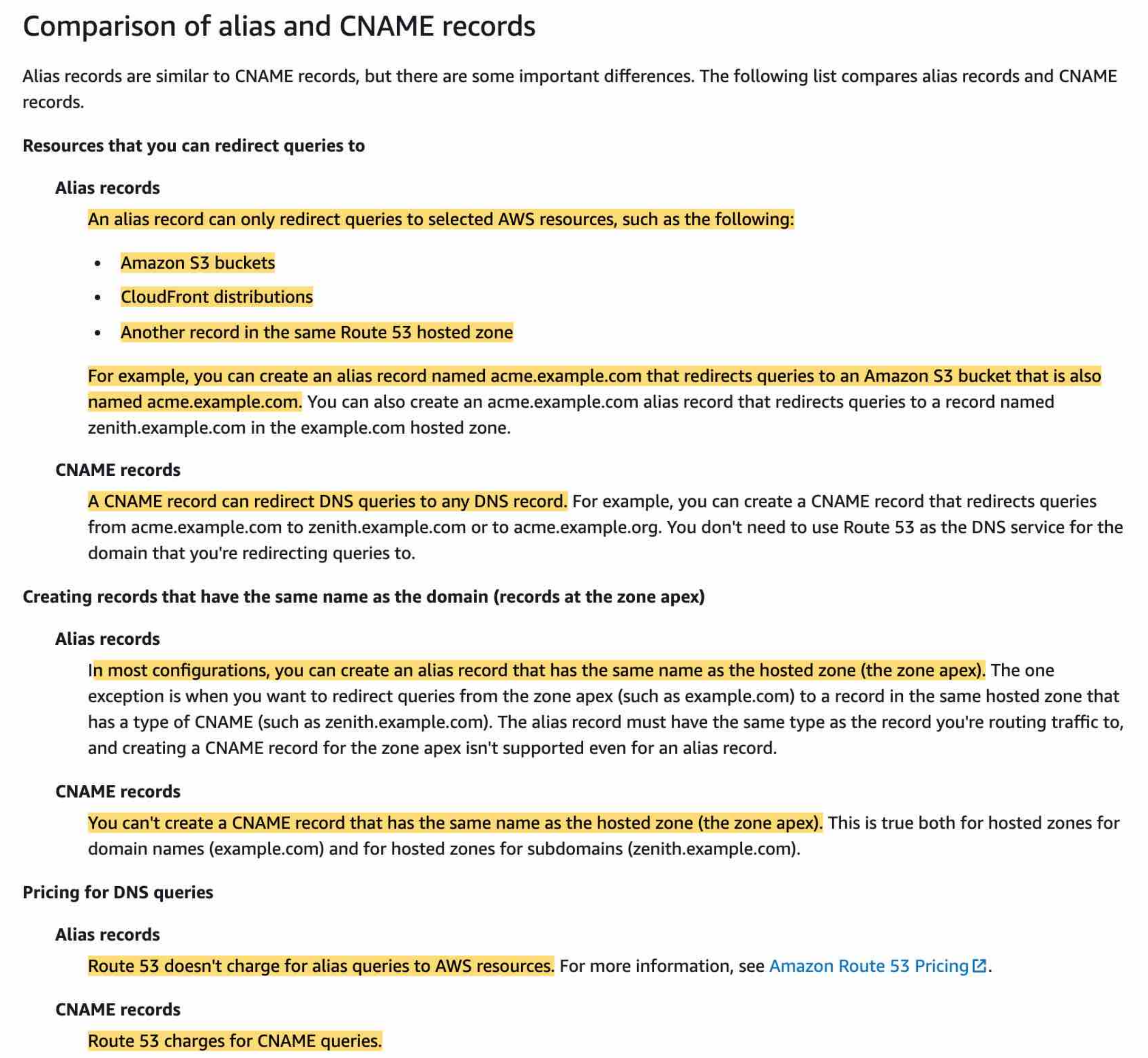
Correct option:

Create a CNAME record

A CNAME record maps DNS queries for the name of the current record, such as acme.example.com, to another domain (example.com or example.net) or subdomain (acme.example.com or zenith.example.org).

CNAME records can be used to map one domain name to another. Although you should keep in mind that the DNS protocol does not allow you to create a CNAME record for the top node of a DNS namespace, also known as the zone apex. For example, if you register the DNS name example.com, the zone apex is example.com. You cannot create a CNAME record for example.com, but you can create CNAME records for www.example.com, newproduct.example.com, and so on.

Please review the major differences between CNAME and Alias Records:



Comparison of alias and CNAME records

Alias records are similar to CNAME records, but there are some important differences. The following list compares alias records and CNAME records.

Resources that you can redirect queries to

Alias records

An alias record can only redirect queries to selected AWS resources, such as the following:

- Amazon S3 buckets
- CloudFront distributions
- Another record in the same Route 53 hosted zone

For example, you can create an alias record named acme.example.com that redirects queries to an Amazon S3 bucket that is also named acme.example.com. You can also create an acme.example.com alias record that redirects queries to a record named zenith.example.com in the example.com hosted zone.

CNAME records

A CNAME record can redirect DNS queries to any DNS record. For example, you can create a CNAME record that redirects queries from acme.example.com to zenith.example.com or to acme.example.org. You don't need to use Route 53 as the DNS service for the domain that you're redirecting queries to.

Creating records that have the same name as the domain (records at the zone apex)

Alias records

In most configurations, you can create an alias record that has the same name as the hosted zone (the zone apex). The one exception is when you want to redirect queries from the zone apex (such as example.com) to a record in the same hosted zone that has a type of CNAME (such as zenith.example.com). The alias record must have the same type as the record you're routing traffic to, and creating a CNAME record for the zone apex isn't supported even for an alias record.

CNAME records

You can't create a CNAME record that has the same name as the hosted zone (the zone apex). This is true both for hosted zones for domain names (example.com) and for hosted zones for subdomains (zenith.example.com).

Pricing for DNS queries

Alias records

Route 53 doesn't charge for alias queries to AWS resources. For more information, see Amazon Route 53 Pricing.

CNAME records

Route 53 charges for CNAME queries.

via - https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html

Incorrect options:

Create an A record - Used to point a domain or subdomain to an IP address. 'A record' cannot be used to map one domain name to another.

Create a PTR record - A Pointer (PTR) record resolves an IP address to a fully-qualified domain name (FQDN) as an opposite to what A record does. PTR records are also called Reverse DNS records. 'PTR record' cannot be used to map one domain name to another.

Create an Alias Record - Alias records let you route traffic to selected AWS resources, such as CloudFront distributions and Amazon S3 buckets. They also let you route traffic from one record in a hosted zone to another record. 3rd party websites do not qualify for these as we have no control over those. 'Alias record' cannot be used to map one domain name to another.

Reference:

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html

Question 15: **Correct**

A healthcare company stores confidential data on an Amazon Simple Storage Service (S3) bucket. New security compliance guidelines require that files be stored with server-side encryption. The encryption used must be Advanced Encryption Standard (AES-256) and the company does not want to manage S3 encryption keys.

Which of the following options should you use?

○ **SSE-KMS**

○ **SSE-S3** **(Correct)**

○ **SSE-C**

○ **Client Side Encryption**

Explanation

Correct option:

SSE-S3

Using Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3), each object is encrypted with a unique key employing strong multi-factor encryption. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.

Incorrect options:

SSE-C - You manage the encryption keys and Amazon S3 manages the encryption as it writes to disks and decryption when you access your objects.

Client-Side Encryption - You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

SSE-KMS - Similar to SSE-S3 and also provides you with an audit trail of when your key was used and by whom. Additionally, you have the option to create and manage encryption keys yourself.

Reference:

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

Question 16: **Incorrect**

An e-commerce company has established a Direct Connect connection between AWS Cloud and their on-premises infrastructure. The development team needs to access the Amazon S3 bucket present in their AWS account to pull the customer data for an application hosted on the on-premises infrastructure.

What is the right way of configuring this requirement?

○ **Create a VPC interface endpoint for the S3 bucket you need to access. Then use the private virtual interface (VIF) using Direct Connect to access the bucket**

○ **Create a dedicated or hosted connection. Establish a cross-network connection and then create a public virtual interface for your connection. Configure an end router for use with the public virtual interface** **(Correct)**

○ **Create a VPC gateway endpoint for the S3 bucket you need to access. Then use the private virtual interface (VIF) using** **(Incorrect)**

Direct Connect to access the bucket

○ **Directly access the S3 bucket through a private virtual interface (VIF) using Direct Connect**

Explanation

Correct option:

Create a dedicated or hosted connection. Establish a cross-network connection and then create a public virtual interface for your connection. Configure an end router for use with the public virtual interface

It's not possible to directly access an S3 bucket through a private virtual interface (VIF) using Direct Connect. This is true even if you have an Amazon Virtual Private Cloud (Amazon VPC) endpoint for Amazon S3 in your VPC because VPC endpoint connections can't extend outside of a VPC. Additionally, Amazon S3 resolves to public IP addresses, even if you enable a VPC endpoint for Amazon S3.

However, you can establish access to Amazon S3 using Direct Connect by following these steps (This configuration doesn't require a VPC endpoint for Amazon S3, because traffic doesn't traverse the VPC):

1. Create a connection. You can request a dedicated connection or a hosted connection.
2. Establish a cross-network connection with the help of your network provider, and then create a public virtual interface for your connection.
3. Configure an end router for use with the public virtual interface.

After the BGP is up and established, the Direct Connect router advertises all global public IP prefixes, including Amazon S3 prefixes. Traffic heading to Amazon S3 is routed through the Direct Connect public virtual interface through a private network connection between AWS and your data center or corporate network.

Incorrect options:

Directly access the S3 bucket through a private virtual interface (VIF) using Direct Connect - Private virtual interface allows access to an Amazon VPC using private IP addresses. It's not possible to directly access an S3 bucket through a private virtual interface (VIF) using Direct Connect.

Create a VPC gateway endpoint for the S3 bucket you need to access. Then use private virtual interface (VIF) using Direct Connect to access the bucket - VPC endpoint connections can't extend outside of a VPC. Additionally, Amazon S3 resolves to public IP addresses, even if you enable a VPC endpoint for Amazon S3.

Create a VPC interface endpoint for the S3 bucket you need to access. Then use private virtual interface (VIF) using Direct Connect to access the bucket - VPC interface endpoint is not used for accessing Amazon S3 buckets, we need to use VPC gateway endpoint. As discussed above, VPC endpoint connections can't extend outside of a VPC. Additionally, Amazon S3 resolves to public IP addresses, even if you enable a VPC endpoint for Amazon S3.

Reference:

https://aws.amazon.com/premiumsupport/knowledge-center/s3-bucket-access-direct-connect/

Question 17: **Correct**

A junior developer is tasked with creating necessary configurations for AWS CloudFormation that is extensively used in a project. After declaring the necessary stack policy, the developer realized that the users still do not have access to stack resources. The stack policy created by the developer looks like so:

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

Why are the users unable to access the stack resources even after giving access permissions to all?

○ A stack policy applies only during stack updates, it doesn't provide access controls. The developer needs to provide access through IAM policies (Correct)

○ Stack policies are associated with a particular IAM role or an IAM user. Hence, they only work for the users you have explicitly attached the policy to

○ Stack policies do not allow wildcard character value (`*`) for the `Principal` element of the policy

○ The stack policy is invalid and hence the users are not granted any permissions. The developer needs to fix the syntactical errors in the policy

Explanation

Correct option:

A stack policy applies only during stack updates, it doesn't provide access controls. The developer needs to provide access through IAM policies - When you create a stack, all update actions are allowed on all resources. By default, anyone with stack update permissions can update all of the resources in the stack. You can prevent stack resources from being unintentionally updated or deleted during a stack update by using a stack policy. A stack policy is a JSON document that defines the update actions that can be performed on designated resources.

After you set a stack policy, all of the resources in the stack are protected by default. To allow updates on specific resources, you specify an explicit Allow statement for those resources in your stack policy. You can define only one stack policy per stack, but, you can protect multiple resources within a single policy.

A stack policy applies only during stack updates. It doesn't provide access controls like an AWS Identity and Access Management (IAM) policy. Use a stack policy only as a fail-safe mechanism to prevent accidental updates to specific stack resources. To control access to AWS resources or actions, use IAM.

Incorrect options:

The stack policy is invalid and hence the users are not granted any permissions. The developer needs to fix the syntactical errors in the policy - This statement is incorrect and given only as a distractor.

Stack policies do not allow wildcard character value (`*`) for the `Principal` element of the policy - The Principal element specifies the entity that the policy applies to. This element is required while creating a policy but supports only the wildcard (*), which means that the policy applies to all principals.

Stack policies are associated with a particular IAM role or an IAM user. Hence, they only work for the users you have explicitly attached the policy to - A stack policy applies to all AWS CloudFormation users who attempt to update the stack. You can't associate different stack policies with different users.

Reference:

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/protect-stack-resources.html

Question 18: **Correct**

A Systems Administrator has just configured an internet facing Load Balancer for traffic distribution across the EC2 instances placed in different Availability Zones. The clients, however, are unable to connect to the Load Balancer.

What is the most plausible reason for this issue?

○ **The target was incorrectly configured as a Lambda function and not an EC2 instance**

○ **The target returned the error code of 200 indicating an error on the server side**

○ **A security group or network ACL is not allowing traffic from the client** **(Correct)**

○ **It is an internal server error**

Explanation

Correct option:

A security group or network ACL is not allowing traffic from the client

If the load balancer is not responding to client requests, check for the following issues:

1. Your internet-facing load balancer may be attached to a private subnet - You must specify public subnets for your load balancer. A public subnet has a route to the Internet Gateway for your virtual private cloud (VPC).
2. A security group or network ACL does not allow traffic - The security group for the load balancer and any network ACLs for the load balancer subnets must allow inbound traffic from the clients and outbound traffic to the clients on the listener ports.

Incorrect options:

It is an internal server error - HTTP 500 is the error code for internal server error, generated by Load Balancer and sent back to the requesting client. But, in the given use case, the client is unable to connect to the Load Balancer itself.

The target returned the error code of 200 indicating an error on the server side - By default, the success code is 200. So, returning an HTTP 200 indicates a successful message.

The target was incorrectly configured as a Lambda function and not an EC2 instance - An ELB can be configured to have a Lambda Function as its target. This should not result in any access issues or errors.

Reference:

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-troubleshooting.html

Question 19: **Correct**

A media company uses S3 to aggregate the raw video footage from its reporting teams across the US. The company has recently expanded into new geographies in Europe and Australia. The technical teams at the overseas branch offices have reported huge delays in uploading large video files to the destination S3 bucket.

Which of the following are the MOST cost-effective options to improve the file upload speed into S3? (Select two)

Use AWS Global Accelerator for faster file uploads into the destination S3 bucket

Use Amazon S3 Transfer Acceleration to enable faster file uploads into the destination S3 bucket **(Correct)**

Use multipart uploads for faster file uploads into the destination S3 bucket (Correct)

Create multiple AWS direct connect connections between the AWS Cloud and branch offices in Europe and Australia. Use the direct connect connections for faster file uploads into S3

Create multiple site-to-site VPN connections between the AWS Cloud and branch offices in Europe and Australia. Use these VPN connections for faster file uploads into S3

Explanation

Correct options:

Use Amazon S3 Transfer Acceleration to enable faster file uploads into the destination S3 bucket - Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. Transfer Acceleration takes advantage of Amazon CloudFront’s globally distributed edge locations. As the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path.

Use multipart uploads for faster file uploads into the destination S3 bucket - Multipart upload allows you to upload a single object as a set of parts. Each part is a contiguous portion of the object's data. You can upload these object parts independently and in any order. If transmission of any part fails, you can retransmit that part without affecting other parts. After all parts of your object are uploaded, Amazon S3 assembles these parts and creates the object. In general, when your object size reaches 100 MB, you should consider using multipart uploads instead of uploading the object in a single operation. Multipart upload provides improved throughput, therefore it facilitates faster file uploads.

Incorrect options:

Create multiple AWS direct connect connections between the AWS Cloud and branch offices in Europe and Australia. Use the direct connect connections for faster file uploads into S3 - AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. AWS Direct Connect lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations.

Direct connect takes significant time (several months) to be provisioned and is an overkill for the given use-case.

Create multiple site-to-site VPN connections between the AWS Cloud and branch offices in Europe and Australia. Use these VPN connections for faster file uploads into S3 - AWS Site-to-Site VPN enables you to securely connect your on-premises network or branch office site to your Amazon Virtual Private Cloud (Amazon VPC). You can securely extend your data center or branch office network to the cloud with an AWS Site-to-Site VPN connection. A VPC VPN Connection utilizes IPSec to establish encrypted network connectivity between your intranet and Amazon VPC over the Internet.

VPN Connections are a good solution if you have low to modest bandwidth requirements and can tolerate the inherent variability in Internet-based connectivity. Site-to-site VPN will not help in accelerating the file transfer speeds into S3 for the given use-case.

Use AWS Global Accelerator for faster file uploads into the destination S3 bucket - AWS Global Accelerator is a service that improves the availability and performance of your applications with local or global users. It provides static IP addresses that act as a fixed entry point to your application endpoints in a single or multiple AWS Regions, such as your Application Load Balancers, Network Load Balancers or Amazon EC2 instances. AWS Global Accelerator will not help in accelerating the file transfer speeds into S3 for the given use-case.

References:

https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html

https://docs.aws.amazon.com/AmazonS3/latest/dev/uploadobjusingmpu.html

Question 20: **Correct**

An e-commerce company manages its IT infrastructure on AWS Cloud via Elastic Beanstalk. The development team at the company is planning to deploy the next version with MINIMUM application downtime and the ability to rollback quickly in case the deployment goes wrong.

As a SysOps Administrator, which of the following options would you recommend to address the given use-case?

○ **Deploy the new application version using 'Rolling' deployment policy**

○ **Deploy the new version to a separate environment via Blue/Green Deployment, and then swap Route 53 records of the two environments to redirect traffic to the new version** **(Correct)**

○ **Deploy the new application version using 'All at once' deployment policy**

○ **Deploy the new application version using 'Rolling with additional batch' deployment policy**

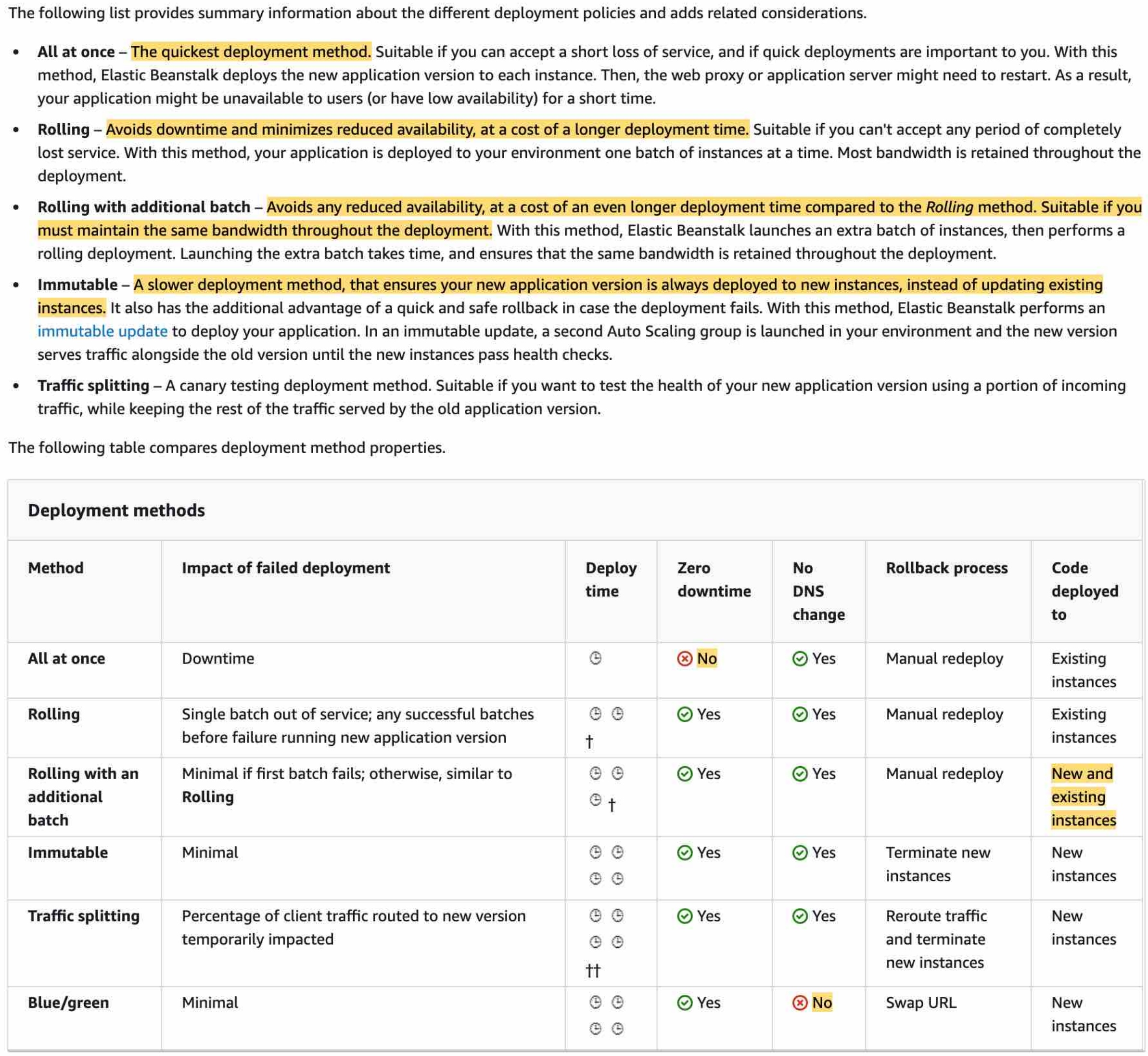
Explanation

Correct option:

Deploy the new version to a separate environment via Blue/Green Deployment, and then swap Route 53 records of the two environments to redirect traffic to the new version

With deployment policies such as 'All at once', AWS Elastic Beanstalk performs an in-place update when you update your application versions and your application can become unavailable to users for a short period of time. You can avoid this downtime by performing a blue/green deployment, where you deploy the new version to a separate environment, and then swap CNAMEs (via Route 53) of the two environments to redirect traffic to the new version instantly. In case of any deployment issues, the rollback process is very quick via swapping the URLs for the two environments.

Overview of Elastic Beanstalk Deployment Policies:



The following list provides summary information about the different deployment policies and adds related considerations.

- **All at once** – The quickest deployment method. Suitable if you can accept a short loss of service, and if quick deployments are important to you. With this method, Elastic Beanstalk deploys the new application version to each instance. Then, the web proxy or application server might need to restart. As a result, your application might be unavailable to users (or have low availability) for a short time.
- **Rolling** – Avoids downtime and minimizes reduced availability, at a cost of a longer deployment time. Suitable if you can't accept any period of completely lost service. With this method, your application is deployed to your environment one batch of instances at a time. Most bandwidth is retained throughout the deployment.
- **Rolling with additional batch** – Avoids any reduced availability, at a cost of an even longer deployment time compared to the *Rolling* method. Suitable if you must maintain the same bandwidth throughout the deployment. With this method, Elastic Beanstalk launches an extra batch of instances, then performs a rolling deployment. Launching the extra batch takes time, and ensures that the same bandwidth is retained throughout the deployment.
- **Immutable** – A slower deployment method, that ensures your new application version is always deployed to new instances, instead of updating existing instances. It also has the additional advantage of a quick and safe rollback in case the deployment fails. With this method, Elastic Beanstalk performs an immutable update to deploy your application. In an immutable update, a second Auto Scaling group is launched in your environment and the new version serves traffic alongside the old version until the new instances pass health checks.
- **Traffic splitting** – A canary testing deployment method. Suitable if you want to test the health of your new application version using a portion of incoming traffic, while keeping the rest of the traffic served by the old application version.

The following table compares deployment method properties.

Deployment methods

Method	Impact of failed deployment	Deploy time	Zero downtime	No DNS change	Rollback process	Code deployed to
All at once	Downtime	🕒	⊗ No	✓ Yes	Manual redeploy	Existing instances
Rolling	Single batch out of service; any successful batches before failure running new application version	🕒 🕒 †	✓ Yes	✓ Yes	Manual redeploy	Existing instances
Rolling with an additional batch	Minimal if first batch fails; otherwise, similar to **Rolling**	🕒 🕒 🕒 †	✓ Yes	✓ Yes	Manual redeploy	New and existing instances
Immutable	Minimal	🕒 🕒 🕒 🕒	✓ Yes	✓ Yes	Terminate new instances	New instances
Traffic splitting	Percentage of client traffic routed to new version temporarily impacted	🕒 🕒 🕒 🕒 ††	✓ Yes	✓ Yes	Reroute traffic and terminate new instances	New instances
Blue/green	Minimal	🕒 🕒 🕒 🕒	✓ Yes	⊗ No	Swap URL	New instances

via - https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.deploy-existing-version.html

Incorrect options:

Deploy the new application version using 'All at once' deployment policy - Although 'All at once' is the quickest deployment method, but the application may become unavailable to users (or have low availability) for a short time. So this option is not correct.

Deploy the new application version using 'Rolling' deployment policy - This policy avoids downtime and minimizes reduced availability, at a cost of a longer deployment time. However rollback process is via manual redeploy, so it's not as quick as the Blue/Green deployment.

Deploy the new application version using 'Rolling with additional batch' deployment policy - This policy avoids any reduced availability, at a cost of an even longer deployment time compared to the Rolling method. Suitable if you must maintain the same bandwidth throughout the deployment. However rollback process is via manual redeploy, so it's not as quick as the Blue/Green deployment.

Reference:

https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.deploy-existing-version.html

Question 21: **Incorrect**

After a developer had mistakenly shutdown a test instance, the Team Lead has decided to configure termination protection on all the instances. As a systems administrator, you have been tasked to review the termination policy and check its viability for the given requirements.

Which of the following choices are correct about Amazon EC2 instance's termination policy (Select two)?

To prevent instances that are part of an Auto Scaling group from terminating on scale in, use instance protection **(Correct)**

The `DisableApiTermination` attribute prevents you from terminating an instance by initiating shutdown from the instance

You can't enable termination protection for Spot Instances (Correct)

The `DisableApiTermination` attribute prevents Amazon EC2 Auto Scaling from terminating an instance (Incorrect)

The `DisableApiTermination` attribute does not prevent you from terminating an instance by initiating shutdown from Amazon EC2 console

Explanation

Correct options:

You can't enable termination protection for Spot Instances - You can't enable termination protection for Spot Instances—a Spot Instance is terminated when the Spot price exceeds the amount you're willing to pay for Spot Instances. However, you can prepare your application to handle Spot Instance interruptions.

To prevent instances that are part of an Auto Scaling group from terminating on scale in, use instance protection - The DisableApiTermination attribute does not prevent Amazon EC2 Auto Scaling from terminating an instance. For instances in an Auto Scaling group, use the following Amazon EC2 Auto Scaling features instead of Amazon EC2 termination protection:

1. To prevent instances that are part of an Auto Scaling group from terminating on scale in, use instance protection.
2. To prevent Amazon EC2 Auto Scaling from terminating unhealthy instances, suspend the ReplaceUnhealthy process.
3. To specify which instances Amazon EC2 Auto Scaling should terminate first, choose a termination policy.

Incorrect options:

The `DisableApiTermination` attribute prevents you from terminating an instance by initiating shutdown from the instance - This is false.
The `DisableApiTermination` attribute does not prevent you from terminating an instance by initiating shutdown from the instance

The `DisableApiTermination` attribute does not prevent you from terminating an instance by initiating shutdown from Amazon EC2 console - By default, you can terminate your instance using the Amazon EC2 console, command line interface, or API. To prevent your instance from being accidentally terminated using Amazon EC2, you can enable termination protection for the instance.

The `DisableApiTermination` attribute prevents Amazon EC2 Auto Scaling from terminating an instance - The `DisableApiTermination` attribute does not prevent Amazon EC2 Auto Scaling from terminating an instance.

Reference:

https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/terminating-instances.html#Using_ChangingDisableAPITermination

Question 22: **Correct**

A financial services firm wants to run its applications on single-tenant hardware to meet security guidelines.

Which of the following is the MOST cost-effective way of isolating the Amazon EC2 instances to a single tenant?

○ **Spot Instances**

○ **On-Demand Instances**

○ **Dedicated Instances** (Correct)

○ **Dedicated Hosts**

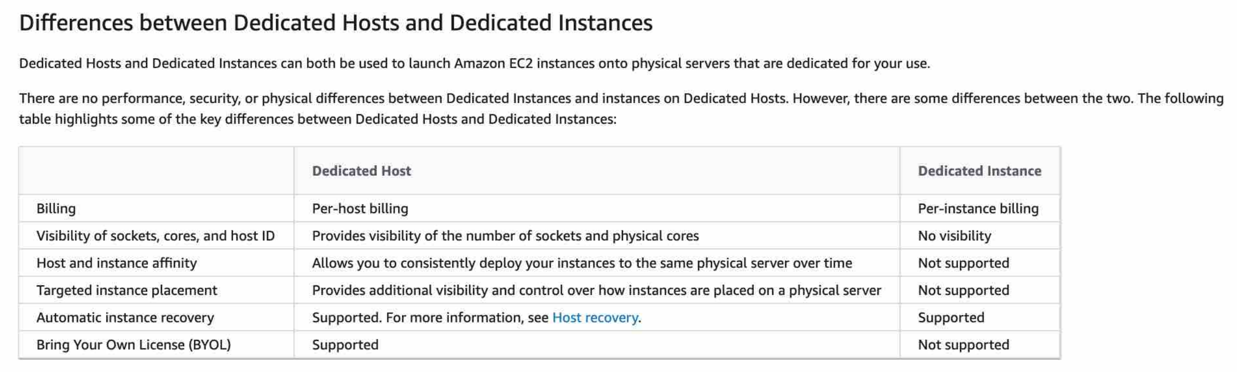
Explanation

Correct option:

Dedicated Instances - Dedicated Instances are Amazon EC2 instances that run in a virtual private cloud (VPC) on hardware that's dedicated to a single customer. Dedicated Instances that belong to different AWS accounts are physically isolated at a hardware level, even if those accounts are linked to a single-payer account. However, Dedicated Instances may share hardware with other instances from the same AWS account that are not Dedicated Instances.

A Dedicated Host is also a physical server that's dedicated for your use. With a Dedicated Host, you have visibility and control over how instances are placed on the server.

Differences between Dedicated Hosts and Dedicated Instances:



Differences between Dedicated Hosts and Dedicated Instances

Dedicated Hosts and Dedicated Instances can both be used to launch Amazon EC2 instances onto physical servers that are dedicated for your use.

There are no performance, security, or physical differences between Dedicated Instances and instances on Dedicated Hosts. However, there are some differences between the two. The following table highlights some of the key differences between Dedicated Hosts and Dedicated Instances:

	Dedicated Host	Dedicated Instance
Billing	Per-host billing	Per-instance billing
Visibility of sockets, cores, and host ID	Provides visibility of the number of sockets and physical cores	No visibility
Host and instance affinity	Allows you to consistently deploy your instances to the same physical server over time	Not supported
Targeted instance placement	Provides additional visibility and control over how instances are placed on a physical server	Not supported
Automatic instance recovery	Supported. For more information, see Host recovery.	Supported
Bring Your Own License (BYOL)	Supported	Not supported

via - https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/dedicated-hosts-overview.html#dedicated-hosts-dedicated-instances

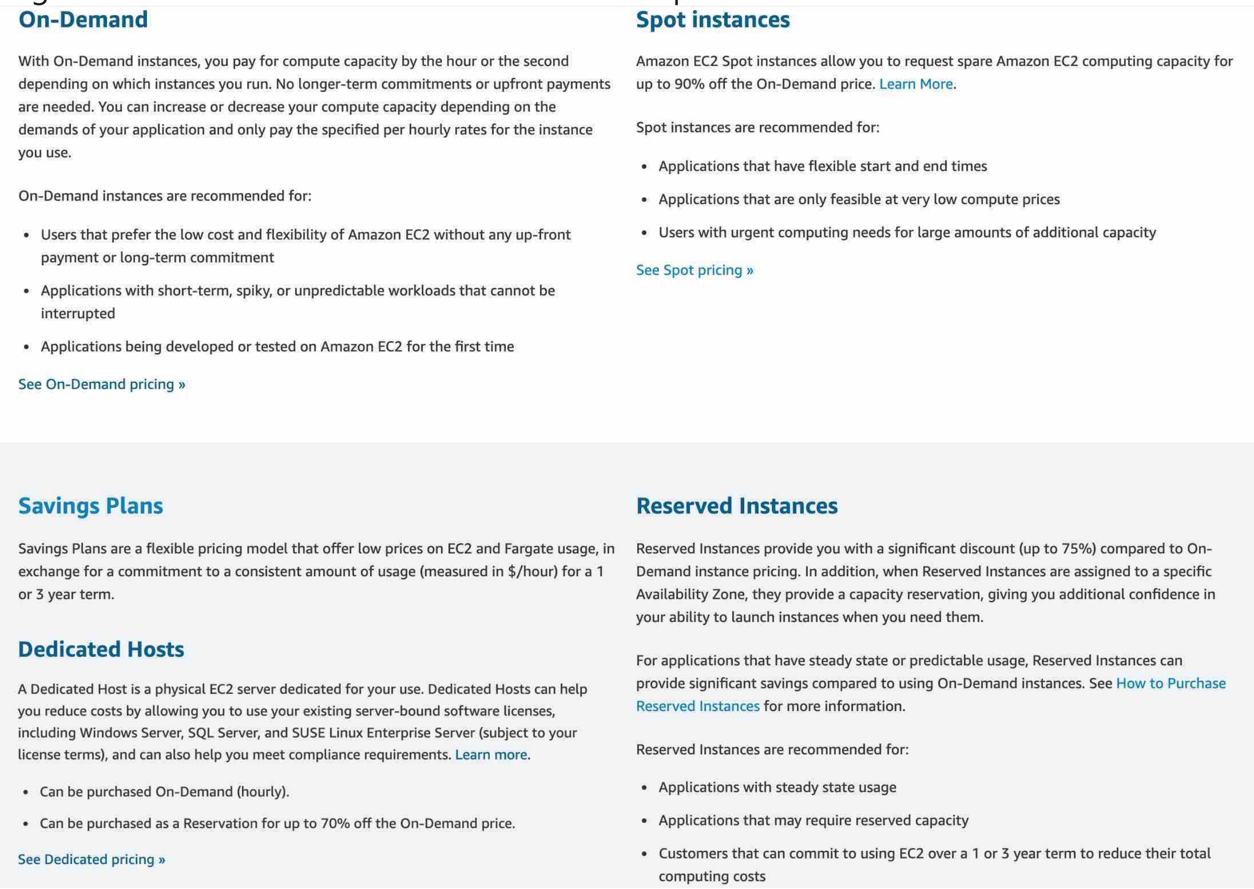
Incorrect options:

Spot Instances - A Spot Instance is an unused EC2 instance that is available for less than the On-Demand price. Your Spot Instance runs whenever capacity is available and the maximum price per hour for your request exceeds the Spot price. Any instance present with unused capacity will be allocated. Even though this is cost-effective, it does not fulfill the single-tenant hardware requirement of the client and hence is not the correct option.

Dedicated Hosts - An Amazon EC2 Dedicated Host is a physical server with EC2 instance capacity fully dedicated to your use. Dedicated Hosts allow you to use your existing software licenses on EC2 instances. With a Dedicated Host, you have visibility and control over how instances are placed on the server. This option is costlier than the Dedicated Instance and hence is not the right choice for the current requirement.

On-Demand Instances - With On-Demand Instances, you pay for the compute capacity by the second with no long-term commitments. You have full control over its lifecycle—you decide when to launch, stop, hibernate, start, reboot, or terminate it. Hardware isolation is not possible and on-demand has one of the costliest instance charges and hence is not the correct answer for current requirements.

High Level Overview of EC2 Instance Purchase Options:



On-Demand

With On-Demand instances, you pay for compute capacity by the hour or the second depending on which instances you run. No longer-term commitments or upfront payments are needed. You can increase or decrease your compute capacity depending on the demands of your application and only pay the specified per hourly rates for the instance you use.

On-Demand instances are recommended for:

- Users that prefer the low cost and flexibility of Amazon EC2 without any up-front payment or long-term commitment
- Applications with short-term, spiky, or unpredictable workloads that cannot be interrupted
- Applications being developed or tested on Amazon EC2 for the first time

See On-Demand pricing »

Spot instances

Amazon EC2 Spot instances allow you to request spare Amazon EC2 computing capacity for up to 90% off the On-Demand price. Learn More.

Spot instances are recommended for:

- Applications that have flexible start and end times
- Applications that are only feasible at very low compute prices
- Users with urgent computing needs for large amounts of additional capacity

See Spot pricing »

Savings Plans

Savings Plans are a flexible pricing model that offer low prices on EC2 and Fargate usage, in exchange for a commitment to a consistent amount of usage (measured in $/hour) for a 1 or 3 year term.

Dedicated Hosts

A Dedicated Host is a physical EC2 server dedicated for your use. Dedicated Hosts can help you reduce costs by allowing you to use your existing server-bound software licenses, including Windows Server, SQL Server, and SUSE Linux Enterprise Server (subject to your license terms), and can also help you meet compliance requirements. Learn more.

- Can be purchased On-Demand (hourly).
- Can be purchased as a Reservation for up to 70% off the On-Demand price.

See Dedicated pricing »

Reserved Instances

Reserved Instances provide you with a significant discount (up to 75%) compared to On-Demand instance pricing. In addition, when Reserved Instances are assigned to a specific Availability Zone, they provide a capacity reservation, giving you additional confidence in your ability to launch instances when you need them.

For applications that have steady state or predictable usage, Reserved Instances can provide significant savings compared to using On-Demand instances. See How to Purchase Reserved Instances for more information.

Reserved Instances are recommended for:

- Applications with steady state usage
- Applications that may require reserved capacity
- Customers that can commit to using EC2 over a 1 or 3 year term to reduce their total computing costs

via - https://aws.amazon.com/ec2/pricing/

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/dedicated-instance.html

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-purchasing-options.html

Question 23: **Correct**

The technology team at a retail company uses CloudFormation to manage its AWS infrastructure. The team has created a network stack containing a VPC with subnets and a web application stack with EC2 instances and an RDS instance. The team wants to reference the VPC created in the network stack into its web application stack.

As a SysOps Administrator, which of the following solutions would you recommend for the given use-case?

○ **Create a cross-stack reference and use the Export output field to flag the value of VPC from the network stack. Then use Ref intrinsic function to reference the value of VPC into the web application stack**

○ **Create a cross-stack reference and use the Export output field to flag the value of VPC from the network stack. Then use Fn::ImportValue intrinsic function to import the value of VPC into the web application stack** **(Correct)**

○ **Create a cross-stack reference and use the Outputs output field to flag the value of VPC from the network stack. Then use Fn::ImportValue intrinsic function to import the value of VPC into the web application stack**

○ **Create a cross-stack reference and use the Outputs output field to flag the value of VPC from the network stack. Then use Ref intrinsic function to reference the value of VPC into the web application stack**

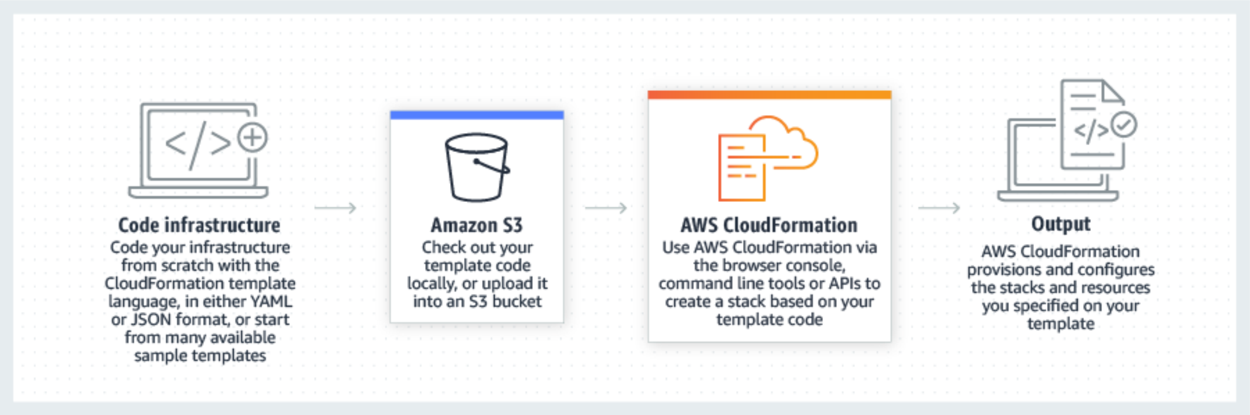
Explanation

Correct option:

Create a cross-stack reference and use the Export output field to flag the value of VPC from the network stack. Then use Fn::ImportValue intrinsic function to import the value of VPC into the web application stack

AWS CloudFormation gives developers and businesses an easy way to create a collection of related AWS and third-party resources and provision them in an orderly and predictable fashion.

How CloudFormation Works:

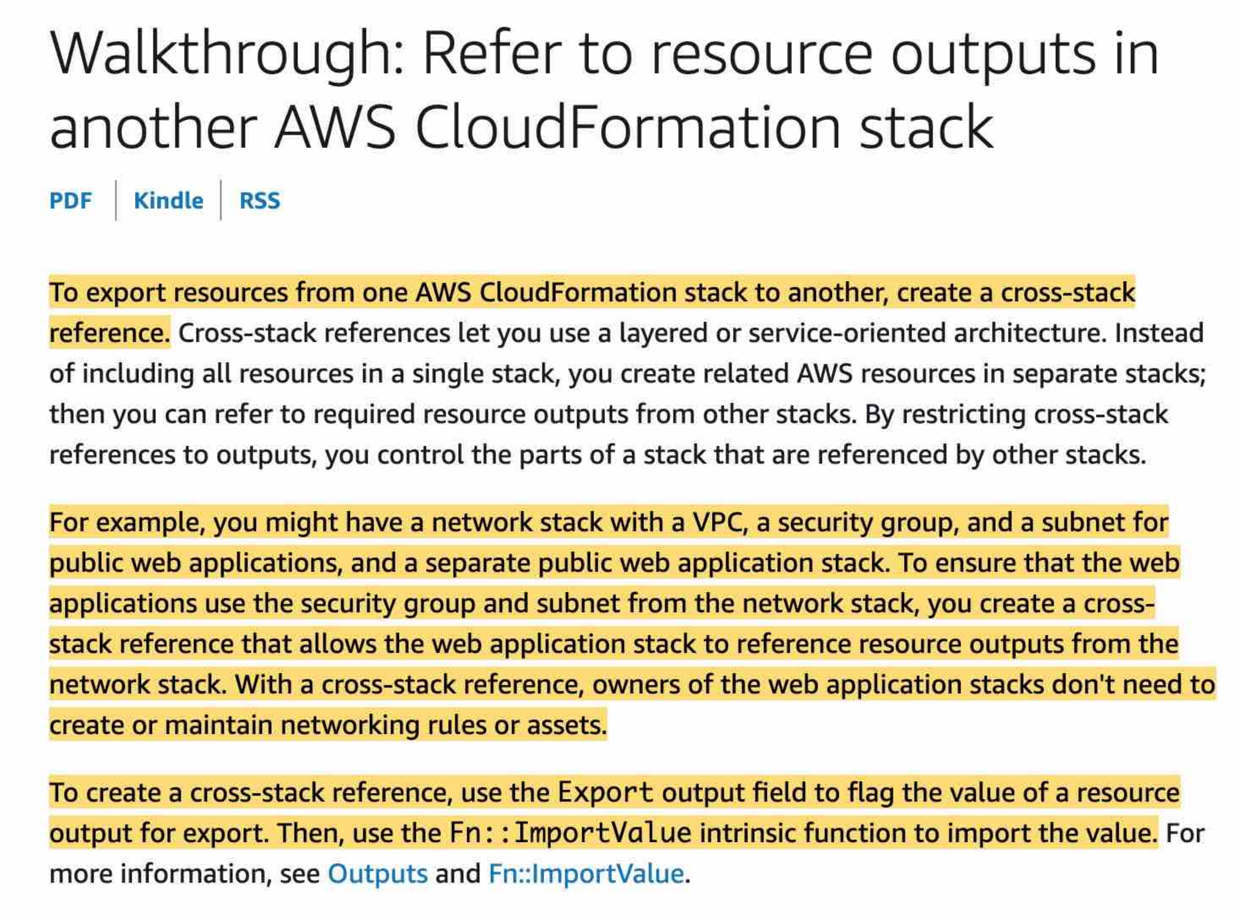

Code infrastructure
Code your infrastructure from scratch with the CloudFormation template language, in either YAML or JSON format, or start from many available sample templates
Amazon S3
Check out your template code locally, or upload it into an S3 bucket
AWS CloudFormation
Use AWS CloudFormation via the browser console, command line tools or APIs to create a stack based on your template code
Output
AWS CloudFormation provisions and configures the stacks and resources you specified on your template

via - https://aws.amazon.com/cloudformation/

You can create a cross-stack reference to export resources from one AWS CloudFormation stack to another. For example, you might have a network stack with a VPC and subnets and a separate public web application stack. To use the security group and subnet from the network stack, you can create a cross-stack reference that allows the web application stack to reference resource outputs from the network stack. With a cross-stack reference, owners of the web application stacks don't need to create or maintain networking rules or assets.

To create a cross-stack reference, use the Export output field to flag the value of a resource output for export. Then, use the Fn::ImportValue intrinsic function to import the value.

You cannot use the Ref intrinsic function to import the value.



Walkthrough: Refer to resource outputs in another AWS CloudFormation stack

To export resources from one AWS CloudFormation stack to another, create a cross-stack reference. Cross-stack references let you use a layered or service-oriented architecture. Instead of including all resources in a single stack, you create related AWS resources in separate stacks; then you can refer to required resource outputs from other stacks. By restricting cross-stack references to outputs, you control the parts of a stack that are referenced by other stacks.

For example, you might have a network stack with a VPC, a security group, and a subnet for public web applications, and a separate public web application stack. To ensure that the web applications use the security group and subnet from the network stack, you create a cross-stack reference that allows the web application stack to reference resource outputs from the network stack. With a cross-stack reference, owners of the web application stacks don't need to create or maintain networking rules or assets.

To create a cross-stack reference, use the `Export` output field to flag the value of a resource output for export. Then, use the `Fn::ImportValue` intrinsic function to import the value. For more information, see Outputs and Fn::ImportValue.

via - https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/walkthrough-crossstackref.html

Incorrect options:

Create a cross-stack reference and use the Outputs output field to flag the value of VPC from the network stack. Then use Fn::ImportValue intrinsic function to import the value of VPC into the web application stack

Create a cross-stack reference and use the Outputs output field to flag the value of VPC from the network stack. Then use Ref intrinsic function to reference the value of VPC into the web application stack

Create a cross-stack reference and use the Export output field to flag the value of VPC from the network stack. Then use Ref intrinsic function to reference the value of VPC into the web application stack

These three options contradict the explanation above, so these options are not correct.

References:

https://aws.amazon.com/cloudformation/

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/walkthrough-crossstackref.html

Question 24: **Correct**

The development team at an e-commerce company uses Amazon MySQL RDS because it simplifies much of the time-consuming administrative tasks typically associated with databases. A new systems administrator has joined the team and wants to understand the replication capabilities for Multi-AZ as well as Read-replicas.

Which of the following correctly summarizes these capabilities for the given database?

○ **Multi-AZ follows asynchronous replication and spans one Availability Zone within a single region. Read replicas follow synchronous replication and can be within an Availability Zone, Cross-AZ, or Cross-Region**

○ **Multi-AZ follows asynchronous replication and spans at least two Availability Zones within a single region. Read replicas follow synchronous replication and can be within an Availability Zone, Cross-AZ, or Cross-Region**

○ **Multi-AZ follows synchronous replication and spans at least two Availability Zones within a single region. Read replicas follow asynchronous replication and can be within an Availability Zone, Cross-AZ, or Cross-Region** **(Correct)**

○ **Multi-AZ follows asynchronous replication and spans at least two Availability Zones within a single region. Read replicas follow**

asynchronous replication and can be within an Availability Zone, Cross-AZ, or Cross-Region

Explanation

Correct option:

Multi-AZ follows synchronous replication and spans at least two Availability Zones within a single region. Read replicas follow asynchronous replication and can be within an Availability Zone, Cross-AZ, or Cross-Region

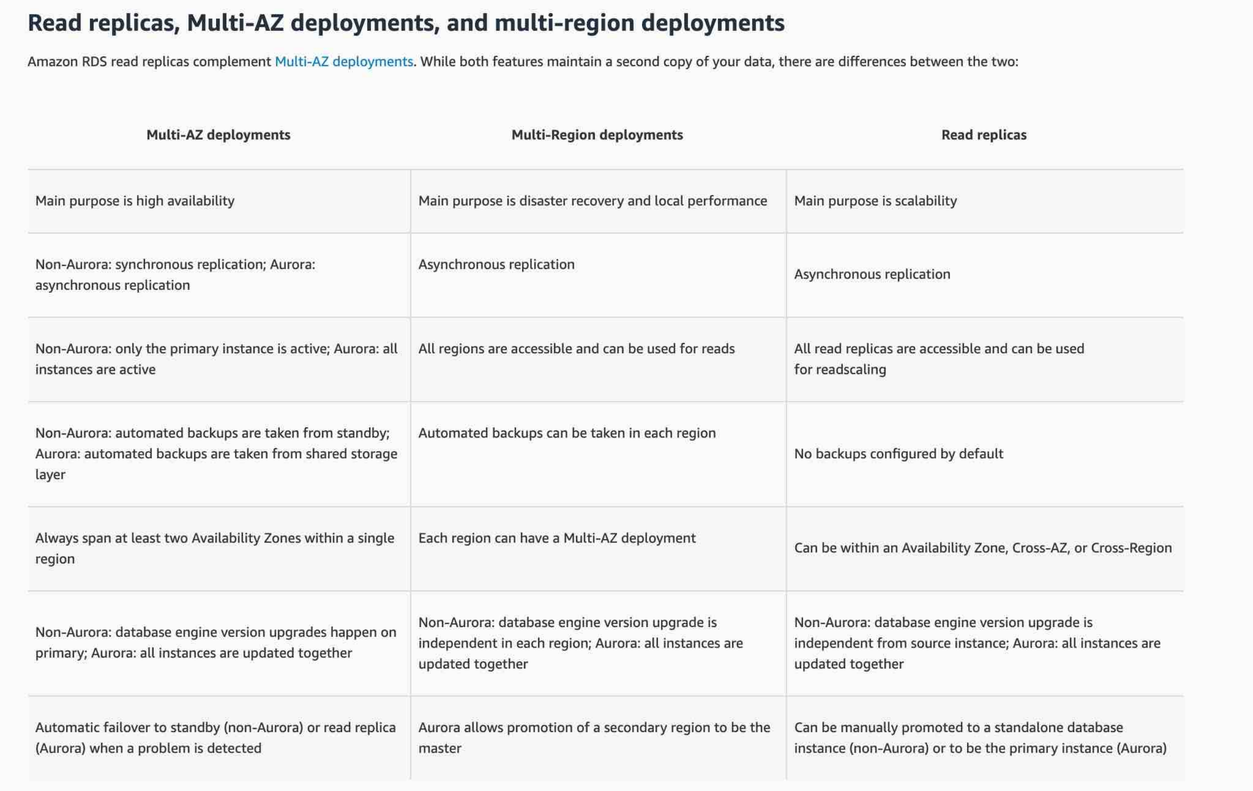
Amazon RDS Multi-AZ deployments provide enhanced availability and durability for RDS database (DB) instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Multi-AZ spans at least two Availability Zones within a single region.

Amazon RDS Read Replicas provide enhanced performance and durability for RDS database (DB) instances. They make it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. For the MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server database engines, Amazon RDS creates a second DB instance using a snapshot of the source DB instance. It then uses the engines' native asynchronous replication to update the read replica whenever there is a change to the source DB instance.

Amazon RDS replicates all databases in the source DB instance. Read replicas can be within an Availability Zone, Cross-AZ, or Cross-Region.

Exam Alert:

Please review this comparison vis-a-vis Multi-AZ vs Read Replica for RDS:



Read replicas, Multi-AZ deployments, and multi-region deployments

Amazon RDS read replicas complement Multi-AZ deployments. While both features maintain a second copy of your data, there are differences between the two:

Multi-AZ deployments	Multi-Region deployments	Read replicas
Main purpose is high availability	Main purpose is disaster recovery and local performance	Main purpose is scalability
Non-Aurora: synchronous replication; Aurora: asynchronous replication	Asynchronous replication	Asynchronous replication
Non-Aurora: only the primary instance is active; Aurora: all instances are active	All regions are accessible and can be used for reads	All read replicas are accessible and can be used for readscaling
Non-Aurora: automated backups are taken from standby; Aurora: automated backups are taken from shared storage layer	Automated backups can be taken in each region	No backups configured by default
Always span at least two Availability Zones within a single region	Each region can have a Multi-AZ deployment	Can be within an Availability Zone, Cross-AZ, or Cross-Region
Non-Aurora: database engine version upgrades happen on primary; Aurora: all instances are updated together	Non-Aurora: database engine version upgrade is independent in each region; Aurora: all instances are updated together	Non-Aurora: database engine version upgrade is independent from source instance; Aurora: all instances are updated together
Automatic failover to standby (non-Aurora) or read replica (Aurora) when a problem is detected	Aurora allows promotion of a secondary region to be the master	Can be manually promoted to a standalone database instance (non-Aurora) or to be the primary instance (Aurora)

via - https://aws.amazon.com/rds/features/multi-az/

Incorrect Options:

Multi-AZ follows asynchronous replication and spans one Availability Zone within a single region. Read replicas follow synchronous replication and can be within an Availability Zone, Cross-AZ, or Cross-Region

Multi-AZ follows asynchronous replication and spans at least two Availability Zones within a single region. Read replicas follow synchronous replication and can be within an Availability Zone, Cross-AZ, or Cross-Region

Multi-AZ follows asynchronous replication and spans at least two Availability Zones within a single region. Read replicas follow asynchronous replication and can be within an Availability Zone, Cross-AZ, or Cross-Region

These three options contradict the explanation above, so these options are incorrect.

References:

https://aws.amazon.com/rds/features/multi-az/

https://aws.amazon.com/rds/features/read-replicas/

Question 25: **Correct**

A developer is trying to access an Amazon S3 bucket for storing the images used by the web application. The S3 bucket has public read access enabled on it. However, when the developer tries to access the bucket, an error pops up - `403 Access Denied`. The confused developer has connected with you to know why he has no access to the public S3 bucket.

As a SysOps Administrator, how will you troubleshoot this issue?

○ **The resource owner which is the AWS account that created the S3 bucket, has access to the bucket. This is an error in creation, delete the S3 bucket and re-create it again**

○ **AWS Organizations service control policy doesn't allow access to Amazon S3 bucket that the developer is trying to access. Service policy needs to be changed using AWS Organizations**

○ **Run the `AWSSupport-TroubleshootS3PublicRead` automation document on AWS Systems Manager to help diagnose issues with accessing objects from a public S3 bucket** **(Correct)**

○ **Explicit deny statement in the bucket policy can cause forbidden-access errors. Check the bucket policy of the S3 bucket**

Explanation

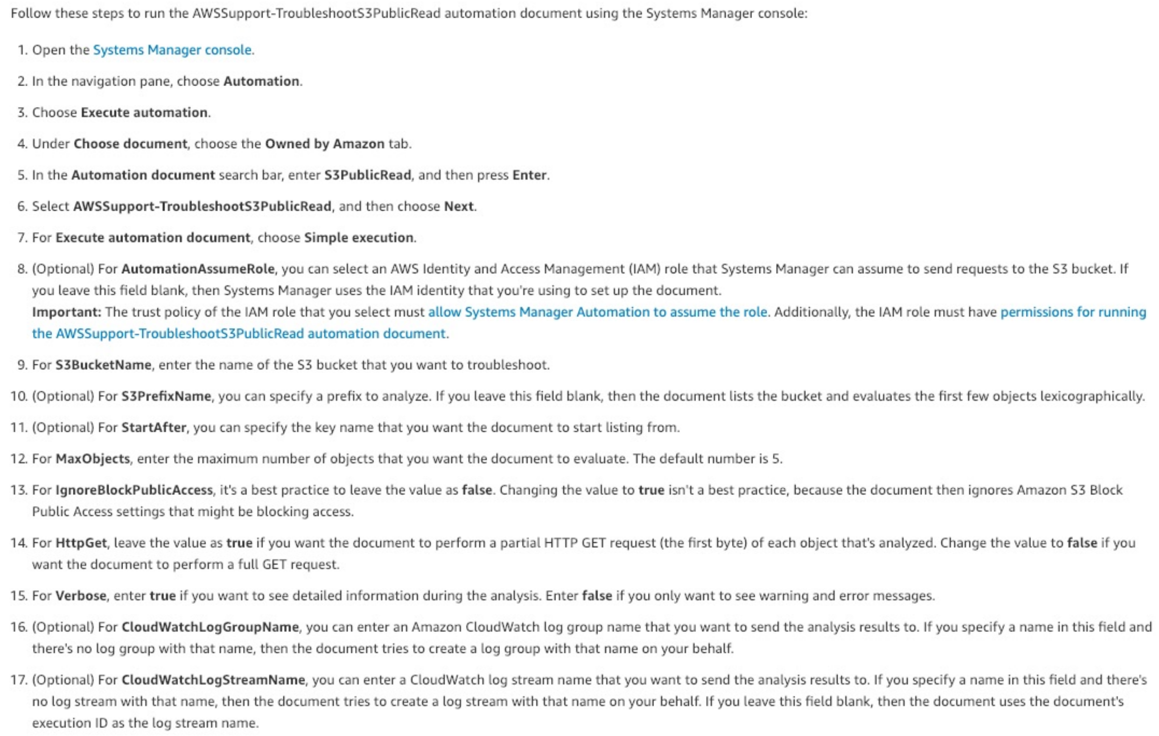
Correct option:

Run the `AWSSupport-TroubleshootS3PublicRead` automation document on AWS Systems Manager to help diagnose issues with accessing objects from a public S3 bucket

Run the `AWSSupport-TroubleshootS3PublicRead` automation document on AWS Systems Manager to help you diagnose issues with accessing objects from a public S3 bucket. This document analyzes some permissions settings that affect the bucket and objects, such as the bucket policy and object access control lists (ACLs), among others.

The `AWSSupport-TroubleshootS3PublicRead` document analyzes 403 errors from publicly readable objects. The document doesn't evaluate permissions for private objects.

Complete Steps to run the AWSSupport-TroubleshootS3PublicRead automation document using the Systems Manager console:



Follow these steps to run the AWSSupport-TroubleshootS3PublicRead automation document using the Systems Manager console:

1. Open the Systems Manager console.
2. In the navigation pane, choose **Automation**.
3. Choose **Execute automation**.
4. Under **Choose document**, choose the **Owned by Amazon** tab.
5. In the **Automation document** search bar, enter **S3PublicRead**, and then press **Enter**.
6. Select **AWSSupport-TroubleshootS3PublicRead**, and then choose **Next**.
7. For **Execute automation document**, choose **Simple execution**.
8. (Optional) For **AutomationAssumeRole**, you can select an AWS Identity and Access Management (IAM) role that Systems Manager can assume to send requests to the S3 bucket. If you leave this field blank, then Systems Manager uses the IAM identity that you're using to set up the document.
   Important: The trust policy of the IAM role that you select must allow Systems Manager Automation to assume the role. Additionally, the IAM role must have permissions for running the AWSSupport-TroubleshootS3PublicRead automation document.
9. For **S3BucketName**, enter the name of the S3 bucket that you want to troubleshoot.
10. (Optional) For **S3PrefixName**, you can specify a prefix to analyze. If you leave this field blank, then the document lists the bucket and evaluates the first few objects lexicographically.
11. (Optional) For **StartAfter**, you can specify the key name that you want the document to start listing from.
12. For **MaxObjects**, enter the maximum number of objects that you want the document to evaluate. The default number is 5.
13. For **IgnoreBlockPublicAccess**, it's a best practice to leave the value as **false**. Changing the value to **true** isn't a best practice, because the document then ignores Amazon S3 Block Public Access settings that might be blocking access.
14. For **HttpGet**, leave the value as **true** if you want the document to perform a partial HTTP GET request (the first byte) of each object that's analyzed. Change the value to **false** if you want the document to perform a full GET request.
15. For **Verbose**, enter **true** if you want to see detailed information during the analysis. Enter **false** if you only want to see warning and error messages.
16. (Optional) For **CloudWatchLogGroupName**, you can enter an Amazon CloudWatch log group name that you want to send the analysis results to. If you specify a name in this field and there's no log group with that name, then the document tries to create a log group with that name on your behalf.
17. (Optional) For **CloudWatchLogStreamName**, you can enter a CloudWatch log stream name that you want to send the analysis results to. If you specify a name in this field and there's no log stream with that name, then the document tries to create a log stream with that name on your behalf. If you leave this field blank, then the document uses the document's execution ID as the log stream name.

via - https://aws.amazon.com/premiumsupport/knowledge-center/s3-troubleshoot-403-public-read/

Incorrect options:

Explicit deny statement in the bucket policy can cause forbidden-access errors. Check the bucket policy of the S3 bucket

AWS Organizations service control policy doesn't allow access to Amazon S3 bucket that the developer is trying to access. Service policy needs to be changed using AWS Organizations

Either of these two options could be true. To know exactly what is causing the error, AWS provides `AWSSupport-TroubleshootS3PublicRead` automation document on AWS Systems Manager. This is the optimal way of troubleshooting the current issue.

The resource owner which is the AWS account that created the S3 bucket, has access to the bucket. This is an error in creation, delete the S3 bucket and re-create it again - It is not mentioned in the use-case if it is the resource owner trying to access the S3 bucket.

Reference:

https://aws.amazon.com/premiumsupport/knowledge-center/s3-troubleshoot-403-public-read/

Question 26: **Correct**

A multi-national retail company wants to explore a hybrid cloud environment with AWS so that it can start leveraging AWS services for some of its daily workflows. The development team at the company wants to establish a dedicated, encrypted, low latency, and high throughput connection between its data center and AWS Cloud. The team has set aside sufficient time to account for the operational overhead of establishing this connection.

As a SysOps Administrator, which of the following solutions would you recommend to the company?

○ **Use AWS Direct Connect to establish a connection between the data center and AWS Cloud**

○ **Use AWS Direct Connect plus VPN to establish a connection between the data center and AWS Cloud** **(Correct)**

○ **Use site-to-site VPN to establish a connection between the data center and AWS Cloud**

○ **Use VPC transit gateway to establish a connection between the data center and AWS Cloud**

Explanation

Correct option:

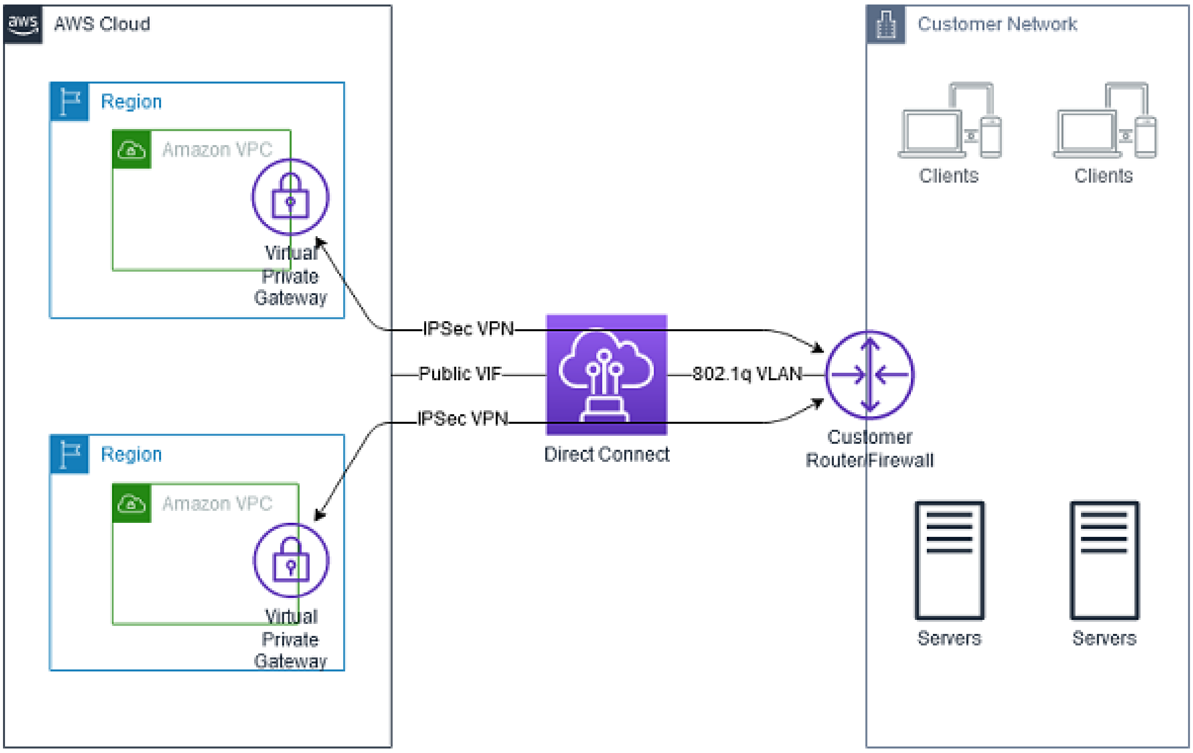
Use AWS Direct Connect plus VPN to establish a connection between the data center and AWS Cloud

AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. AWS Direct Connect lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations.

With AWS Direct Connect plus VPN, you can combine one or more AWS Direct Connect dedicated network connections with the Amazon VPC VPN. This combination provides an IPsec-encrypted private connection that also reduces network costs, increases bandwidth throughput, and provides a more consistent network experience than internet-based VPN connections.

This solution combines the AWS managed benefits of the VPN solution with low latency, increased bandwidth, more consistent benefits of the AWS Direct Connect solution, and an end-to-end, secure IPsec connection. Therefore, AWS Direct Connect plus VPN is the correct solution for this use-case.

AWS Direct Connect Plus VPN:



via

- https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-vpn.html

Incorrect options:

Use site-to-site VPN to establish a connection between the data center and AWS Cloud - AWS Site-to-Site VPN enables you to securely connect your on-premises network or branch office site to your Amazon Virtual Private Cloud (Amazon VPC). A VPC VPN Connection utilizes IPSec to establish encrypted network connectivity between your intranet and Amazon VPC over the Internet. VPN Connections are a good solution if you have an immediate need, have low to modest bandwidth requirements, and can tolerate the inherent variability in Internet-based connectivity.

However, Site-to-site VPN cannot provide low latency and high throughput connection, therefore this option is ruled out.

Use VPC transit gateway to establish a connection between the data center and AWS Cloud - A transit gateway is a network transit hub that you can use to interconnect your virtual private clouds (VPC) and on-premises networks. A transit gateway by itself cannot establish a low latency and high throughput connection between a data center and AWS Cloud. Hence this option is incorrect.

Use AWS Direct Connect to establish a connection between the data center and AWS Cloud - AWS Direct Connect by itself cannot provide an encrypted connection between a data center and AWS Cloud, so this option is ruled out.

References:

https://aws.amazon.com/directconnect/

https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-plus-vpn-network-to-amazon.html

Question 27: **Correct**

A developer is tasked with cleaning up obsolete resources. When he tried to delete an AWS CloudFormation stack, the stack deletion process returned without any error or a success message. The stack was not deleted either.

What is the reason for this behavior and how will you fix it?

○ **Dependent resources should be deleted first, before deleting the rest of the resources in the stack. If this order is not followed, then stack deletion fails without an error**

○ **Some resources must be empty before they can be deleted. Such resources will not be deleted if they are not empty and stack deletion fails without any error**

○ **If you attempt to delete a stack with termination protection enabled, the deletion fails and the stack - including its status - remains unchanged** **(Correct)**

○ **The AWS user who initiated the stack deletion does not have enough permissions**

Explanation

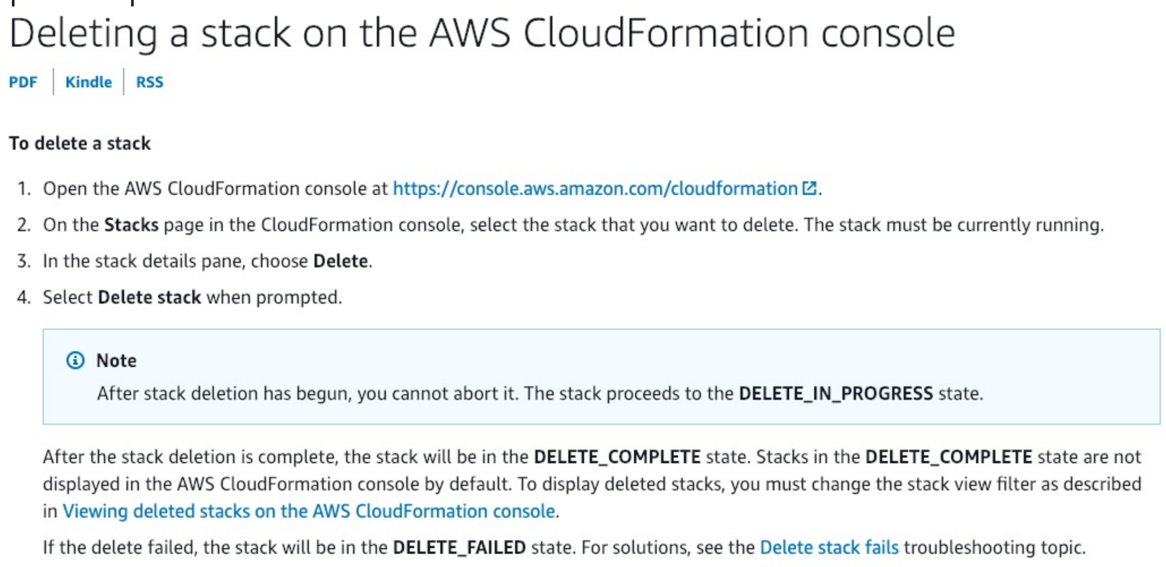
Correct option:

If you attempt to delete a stack with termination protection enabled, the deletion fails and the stack - including its status - remains unchanged

You cannot delete stacks that have termination protection enabled. If you attempt to delete a stack with termination protection enabled, the deletion fails and the stack - including its status - remains unchanged. Disable termination protection on the stack, then perform the delete operation again.

This includes nested stacks whose root stacks have termination protection enabled. Disable termination protection on the root stack, then perform the delete operation again. It is strongly recommended that you do not delete nested stacks directly, but only delete them as part of deleting the root stack and all its resources.

Complete steps for Stack deletion:



Deleting a stack on the AWS CloudFormation console

PDF | Kindle | RSS

To delete a stack

1. Open the AWS CloudFormation console at https://console.aws.amazon.com/cloudformation.
2. On the **Stacks** page in the CloudFormation console, select the stack that you want to delete. The stack must be currently running.
3. In the stack details pane, choose **Delete**.
4. Select **Delete stack** when prompted.

> **Note**
>
> After stack deletion has begun, you cannot abort it. The stack proceeds to the **DELETE_IN_PROGRESS** state.

After the stack deletion is complete, the stack will be in the **DELETE_COMPLETE** state. Stacks in the **DELETE_COMPLETE** state are not displayed in the AWS CloudFormation console by default. To display deleted stacks, you must change the stack view filter as described in Viewing deleted stacks on the AWS CloudFormation console.

If the delete failed, the stack will be in the **DELETE_FAILED** state. For solutions, see the Delete stack fails troubleshooting topic.

via - https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-delete-stack.html

Incorrect options:

The AWS user who initiated the stack deletion does not have enough permissions - If the user does not have enough permissions to delete the stack, an error explaining the same is displayed and the stack will be in the DELETE_FAILED state.

Some resources must be empty before they can be deleted. Such resources will not be deleted if they are not empty and stack deletion fails without any error - Some resources must be empty before they can be deleted. For example, you must delete all objects in an Amazon S3 bucket or remove all instances in an Amazon EC2 security group before you can delete the bucket or security group. Otherwise, stack deletion fails and the stack will be in the DELETE_FAILED state.

Dependent resources should be deleted first, before deleting the rest of the resources in the stack. If this order is not followed, then stack deletion fails without an error - Any error during stack deletion will result in the stack being in the DELETE_FAILED state.

Reference:

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/troubleshooting.html

Question 28: **Correct**

An e-commerce company runs their database workloads on Provisioned IOPS SSD (io1) volumes.

As a SysOps Administrator, which of the following options would you identify as an INCORRECT configuration for io1 EBS volume types?

○ **100 GiB size volume with 1000 IOPS**

○ **100 GiB size volume with 5000 IOPS**

○ **100 GiB size volume with 3000 IOPS**

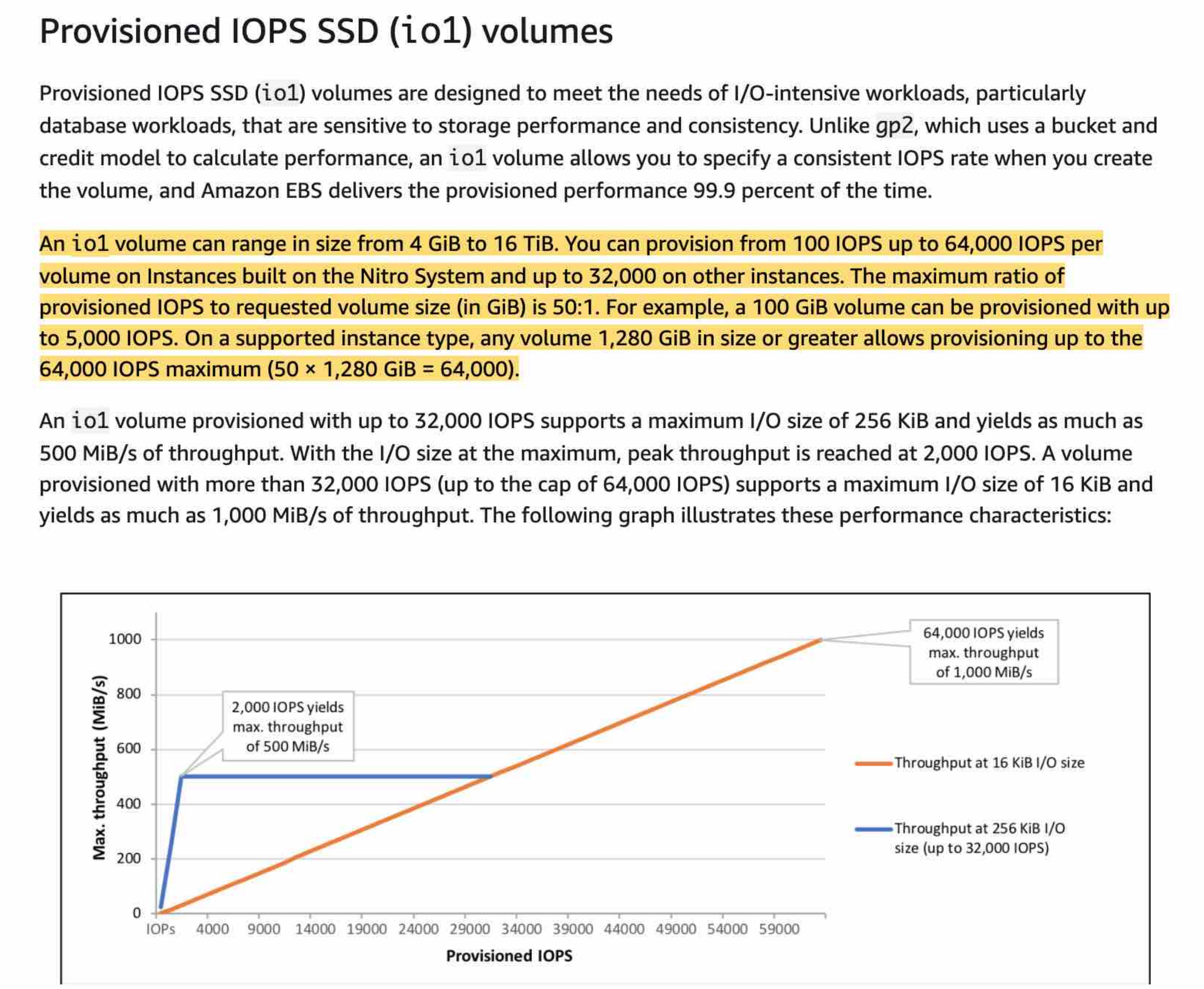
○ **100 GiB size volume with 7500 IOPS** **(Correct)**

Explanation

Correct option:

100 GiB size volume with 7500 IOPS - This is an incorrect configuration. The maximum ratio of provisioned IOPS to the requested volume size (in GiB) is 50:1. So, for a 100 GiB volume size, the max IOPS possible is 100*50 = 5000 IOPS.

Overview of Provisioned IOPS SSD (io1) volumes:



Provisioned IOPS SSD (io1) volumes

Provisioned IOPS SSD (io1) volumes are designed to meet the needs of I/O-intensive workloads, particularly database workloads, that are sensitive to storage performance and consistency. Unlike gp2, which uses a bucket and credit model to calculate performance, an io1 volume allows you to specify a consistent IOPS rate when you create the volume, and Amazon EBS delivers the provisioned performance 99.9 percent of the time.

An io1 volume can range in size from 4 GiB to 16 TiB. You can provision from 100 IOPS up to 64,000 IOPS per volume on Instances built on the Nitro System and up to 32,000 on other instances. The maximum ratio of provisioned IOPS to requested volume size (in GiB) is 50:1. For example, a 100 GiB volume can be provisioned with up to 5,000 IOPS. On a supported instance type, any volume 1,280 GiB in size or greater allows provisioning up to the 64,000 IOPS maximum (50 × 1,280 GiB = 64,000).

An io1 volume provisioned with up to 32,000 IOPS supports a maximum I/O size of 256 KiB and yields as much as 500 MiB/s of throughput. With the I/O size at the maximum, peak throughput is reached at 2,000 IOPS. A volume provisioned with more than 32,000 IOPS (up to the cap of 64,000 IOPS) supports a maximum I/O size of 16 KiB and yields as much as 1,000 MiB/s of throughput. The following graph illustrates these performance characteristics:

Max. throughput (MiB/s)
1000
800
600
400
200
0
IOPs
4000
9000
14000
19000
24000
29000
34000
39000
44000
49000
54000
59000
Provisioned IOPS
2,000 IOPS yields max. throughput of 500 MiB/s
64,000 IOPS yields max. throughput of 1,000 MiB/s
Throughput at 16 KiB I/O size
Throughput at 256 KiB I/O size (up to 32,000 IOPS)

via - https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html

Incorrect options:

Provisioned IOPS SSD (io1) volumes allow you to specify a consistent IOPS rate when you create the volume, and Amazon EBS delivers the provisioned performance 99.9 percent of the time. An io1 volume can range in size from 4 GiB to 16 TiB. The maximum ratio of provisioned IOPS to the requested volume size (in GiB) is 50:1. For example, a 100 GiB volume can be provisioned with up to 5,000 IOPS.

100 GiB size volume with 1000 IOPS - As explained above, up to 5000 IOPS is a valid configuration for the given use-case.

100 GiB size volume with 5000 IOPS - As explained above, up to 5000 IOPS is a valid configuration for the given use-case.

100 GiB size volume with 3000 IOPS - As explained above, up to 5000 IOPS is a valid configuration for the given use-case.

Reference:

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

Question 29: **Correct**

A Silicon Valley based startup uses Elastic Beanstalk to manage its IT infrastructure on AWS Cloud and it would like to deploy the new application version to the EC2 instances. When the deployment is executed, some instances should serve requests with the old application version, while other instances should serve requests using the new application version until the deployment is completed.

Which deployment meets this requirement without incurring additional costs?

○ **Rolling** **(Correct)**

○ **Rolling with additional batches**

○ **All at once**

○ **Immutable**

Explanation

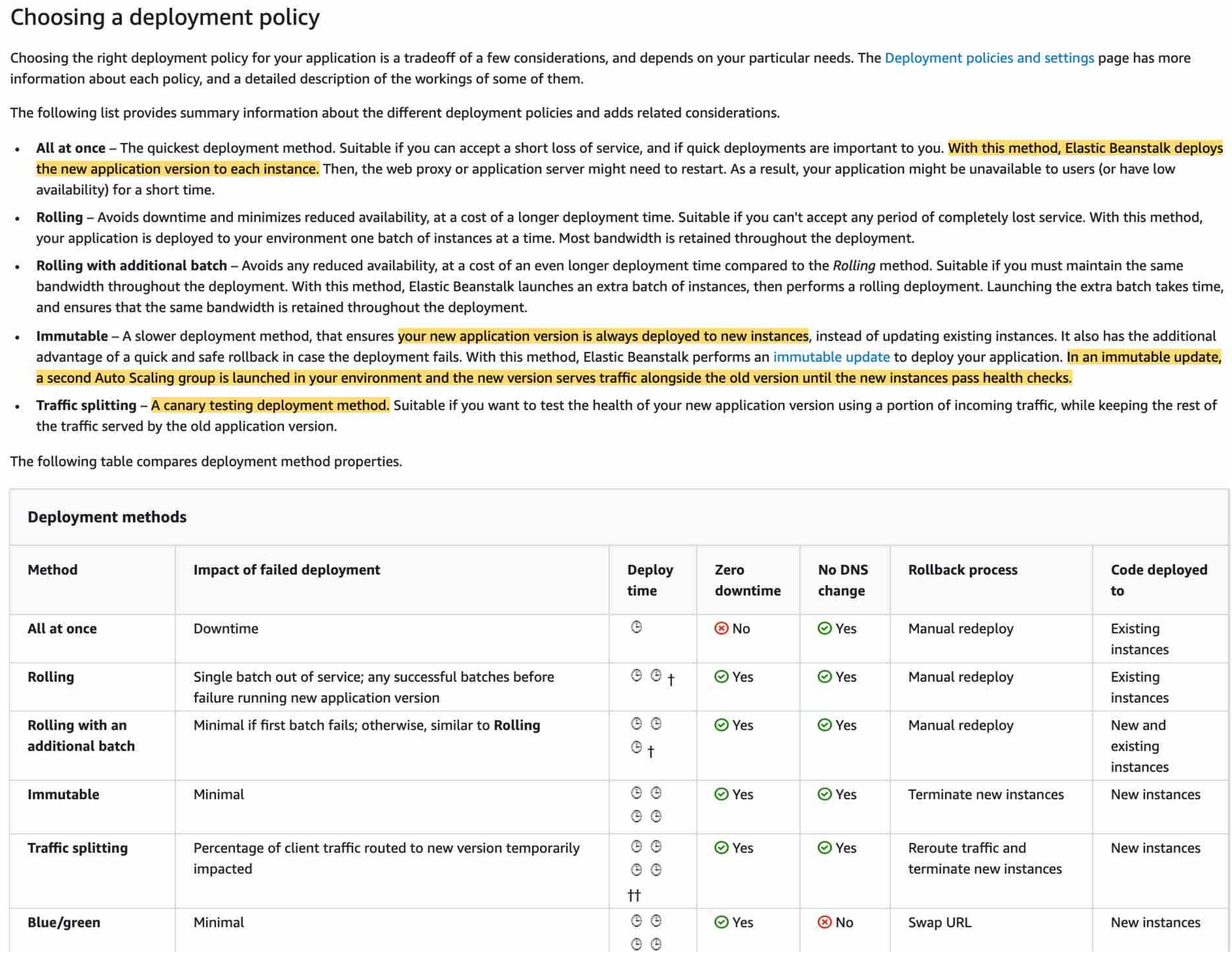
Correct option:

Rolling

With Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without having to learn about the infrastructure that runs those applications. Elastic Beanstalk reduces management complexity without restricting choice or control. You simply upload your application, and Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring.

The rolling deployment policy deploys the new version in batches. Each batch is taken out of service during the deployment phase, reducing your environment's capacity by the number of instances in a batch. The cost remains the same as the number of EC2 instances does not increase. This policy avoids downtime and minimizes reduced availability, at a cost of a longer deployment time.

Overview of Elastic Beanstalk Deployment Policies:



Choosing a deployment policy

Choosing the right deployment policy for your application is a tradeoff of a few considerations, and depends on your particular needs. The Deployment policies and settings page has more information about each policy, and a detailed description of the workings of some of them.

The following list provides summary information about the different deployment policies and adds related considerations.

- **All at once** – The quickest deployment method. Suitable if you can accept a short loss of service, and if quick deployments are important to you. With this method, Elastic Beanstalk deploys the new application version to each instance. Then, the web proxy or application server might need to restart. As a result, your application might be unavailable to users (or have low availability) for a short time.
- **Rolling** – Avoids downtime and minimizes reduced availability, at a cost of a longer deployment time. Suitable if you can't accept any period of completely lost service. With this method, your application is deployed to your environment one batch of instances at a time. Most bandwidth is retained throughout the deployment.
- **Rolling with additional batch** – Avoids any reduced availability, at a cost of an even longer deployment time compared to the *Rolling* method. Suitable if you must maintain the same bandwidth throughout the deployment. With this method, Elastic Beanstalk launches an extra batch of instances, then performs a rolling deployment. Launching the extra batch takes time, and ensures that the same bandwidth is retained throughout the deployment.
- **Immutable** – A slower deployment method, that ensures your new application version is always deployed to new instances, instead of updating existing instances. It also has the additional advantage of a quick and safe rollback in case the deployment fails. With this method, Elastic Beanstalk performs an immutable update to deploy your application. In an immutable update, a second Auto Scaling group is launched in your environment and the new version serves traffic alongside the old version until the new instances pass health checks.
- **Traffic splitting** – A canary testing deployment method. Suitable if you want to test the health of your new application version using a portion of incoming traffic, while keeping the rest of the traffic served by the old application version.

The following table compares deployment method properties.

Deployment methods

Method	Impact of failed deployment	Deploy time	Zero downtime	No DNS change	Rollback process	Code deployed to
All at once	Downtime	🕒	⊗ No	✓ Yes	Manual redeploy	Existing instances
Rolling	Single batch out of service; any successful batches before failure running new application version	🕒 🕒 †	✓ Yes	✓ Yes	Manual redeploy	Existing instances
Rolling with an additional batch	Minimal if first batch fails; otherwise, similar to **Rolling**	🕒 🕒 🕒 †	✓ Yes	✓ Yes	Manual redeploy	New and existing instances
Immutable	Minimal	🕒 🕒 🕒 🕒	✓ Yes	✓ Yes	Terminate new instances	New instances
Traffic splitting	Percentage of client traffic routed to new version temporarily impacted	🕒 🕒 🕒 🕒 ††	✓ Yes	✓ Yes	Reroute traffic and terminate new instances	New instances
Blue/green	Minimal	🕒 🕒 🕒 🕒	✓ Yes	⊗ No	Swap URL	New instances

via - https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.deploy-existing-version.html

Incorrect options:

Immutable - The 'Immutable' deployment policy ensures that your new application version is always deployed to new instances, instead of updating existing instances. It also has the additional advantage of a quick and safe rollback in case the deployment fails.

All at once - This policy deploys the new version to all instances simultaneously. Although 'All at once' is the quickest deployment method, but the application may become unavailable to users (or have low availability) for a short time.

Rolling with additional batches - This policy deploys the new version in batches, but first launches a new batch of instances to ensure full capacity during the deployment process. This policy avoids any reduced availability, at a cost of an even longer deployment time compared to the Rolling method. Suitable if you must maintain the same bandwidth throughout the deployment. These increase the costs as you're adding extra instances during the deployment.

Reference:

https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.deploy-existing-version.html

Question 30: **Correct**

An organization that started as a single AWS account, gradually moved to a multi-account setup. The organization also has multiple AWS environments in each account, that were being managed at the account level. Backups are a big part of this management task. The organization is looking at moving to a centralized backup management process that consolidates and automates Cross-Region backup tasks across AWS accounts.

Which of the solutions below is the right choice for this requirement?

○ **Use Amazon Data Lifecycle Manager to manage creation, deletion, and managing of all the AWS resources under an account. Tag all the resources that need to be backed up and use lifecycle policies to customize the backup management to cater to the needs of the organization**

○ Use Amazon EventBridge to create a workflow for scheduled backup of all AWS resources under an account. Amazon S3 lifecycle policies, Amazon EC2 instance backups, and Amazon RDS backups can be used to create the events for the EventBridge. The same workflow can be scheduled to work on production and non-production environments, based on the tags created

○ Configure AWS Systems Manager Maintenance Windows to schedule backup tasks as per company's policies. Tag the resources to help identify them by the AWS environment they run in. Amazon CloudWatch dashboards hosted by Systems Manager to get an overall view of the status of all resources under the AWS account

○ Create a backup plan in AWS Backup. Assign tags to resources based on the environment (Production, Development, Testing). Create one backup policy for production environments and one backup policy for non-production environments. Schedule the backup plan based

(Correct)

on the organization's backup policies

Explanation

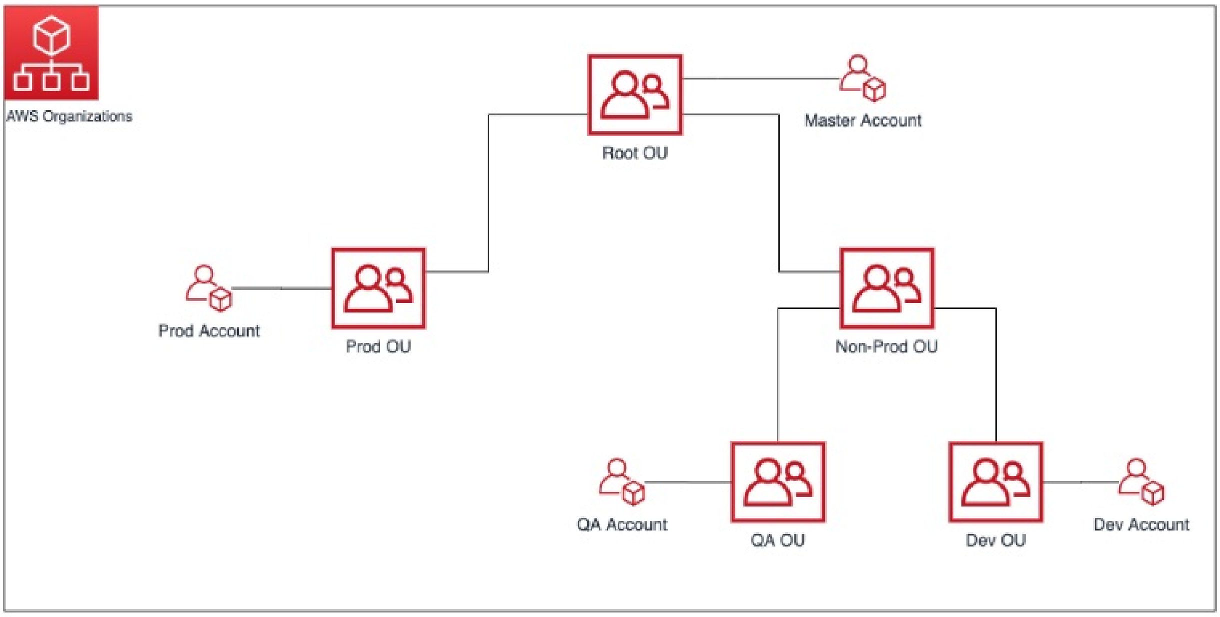
Correct option:

Create a backup plan in AWS Backup. Assign tags to resources based on the environment (Production, Development, Testing). Create one backup policy for production environments and one backup policy for non-production environments. Schedule the backup plan based on the organization's backup policies

AWS Backup is a fully managed and cost-effective backup service that simplifies and automates data backup across AWS services including Amazon EBS, Amazon EC2, Amazon RDS, Amazon Aurora, Amazon DynamoDB, Amazon EFS, and AWS Storage Gateway. In addition, AWS Backup leverages AWS Organizations to implement and maintain a central view of backup policy across resources in a multi-account AWS environment. Customers simply tag and associate their AWS resources with backup policies managed by AWS Backup for Cross-Region data replication.

The following post shows how to centrally manage backup tasks across AWS accounts in your organization by deploying backup policies with AWS Backup.

Example AWS Backup Architecture:



via - https://aws.amazon.com/blogs/storage/centralized-cross-account-management-with-cross-region-copy-using-aws-backup/

Incorrect options:

Configure AWS Systems Manager Maintenance Windows to schedule backup tasks as per the company's policies. Tag the resources to help identify them by the AWS environment they run in. Amazon CloudWatch dashboards hosted by Systems Manager to get an overall view of the status of all resources under the AWS account

AWS Systems Manager Maintenance Windows let you define a schedule for when to perform potentially disruptive actions on your instances such as patching an operating system, updating drivers, or installing software or patches. Although a useful service, it is not suited for the given requirements.

Use Amazon EventBridge to create a workflow for scheduled backup of all AWS resources under an account. Amazon S3 lifecycle policies, Amazon EC2 instance backups, and Amazon RDS backups can be used to create the events for the EventBridge. The same workflow can be scheduled to work on production and non-production environments, based on the tags created - Amazon EventBridge is a serverless event bus that makes it easy to connect applications together using data from your own applications, integrated Software-as-a-Service (SaaS) applications, and AWS services. It is possible to build a backup solution using EventBridge, but it will not be an optimized one, since AWS offers services with better features for centrally managing backups.

Use Amazon Data Lifecycle Manager to manage creation, deletion and managing of all the AWS resources under an account. Tag all the resources that need to be backed up and use lifecycle policies to customize the backup management to cater to the needs of the organization - DLM provides a simple way to manage the lifecycle of EBS resources, such as volume snapshots. You should use DLM when you want to automate the creation, retention, and deletion of EBS snapshots.

References:

https://aws.amazon.com/blogs/storage/centralized-cross-account-management-with-cross-region-copy-using-aws-backup/

https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-maintenance.html

https://aws.amazon.com/eventbridge/

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-lifecycle.html

Question 31: **Correct**

A video streaming solutions provider is migrating to AWS Cloud infrastructure for delivering its content to users across the world. The company wants to make sure that the solution supports at least a million requests per second for its EC2 server farm.

As a SysOps Administrator, which type of Elastic Load Balancer would you recommend as part of the solution stack?

○ **Network Load Balancer** **(Correct)**

○ **Infrastructure Load Balancer**

○ **Application Load Balancer**

○ **Classic Load Balancer**

Explanation

Correct option:

Network Load Balancer

Network Load Balancer is best suited for use-cases involving low latency and high throughput workloads that involve scaling to millions of requests per second. Network Load Balancer operates at the connection level (Layer 4), routing connections to targets - Amazon EC2 instances, microservices, and containers – within Amazon Virtual Private Cloud (Amazon VPC) based on IP protocol data.

Incorrect options:

Application Load Balancer - Application Load Balancer operates at the request level (layer 7), routing traffic to targets – EC2 instances, containers, IP addresses, and Lambda functions based on the content of the request. Ideal for advanced load balancing of HTTP and HTTPS traffic, Application Load Balancer provides advanced request routing targeted at the delivery of modern application architectures, including microservices and container-based applications.

Application Load Balancer is not a good fit for the low latency and high throughput scenario mentioned in the given use-case.

Classic Load Balancer - Classic Load Balancer provides basic load balancing across multiple Amazon EC2 instances and operates at both the request level and connection level. Classic Load Balancer is intended for applications that were built within the EC2-Classic network. Classic Load Balancer is not a good fit for the low latency and high throughput scenario mentioned in the given use-case.

Infrastructure Load Balancer - There is no such thing as Infrastructure Load Balancer and this option just acts as a distractor.

Reference:

https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html

Question 32: **Correct**

A SysOps Administrator was asked to enable versioning on an Amazon S3 bucket after a few objects were accidentally deleted by the development team.

Which of the following represent valid scenarios when a developer deletes an object in the versioning-enabled bucket? (Select two)

□ **GET requests can retrieve delete marker objects**

□ **The delete marker has the same data associated with it, as the actual object**

□ **A delete marker has a key, version ID and Access Control List (ACL) associated with it**

GET requests do not retrieve delete marker objects (Correct)

A delete marker is set on the deleted object, but the actual object is not deleted (Correct)

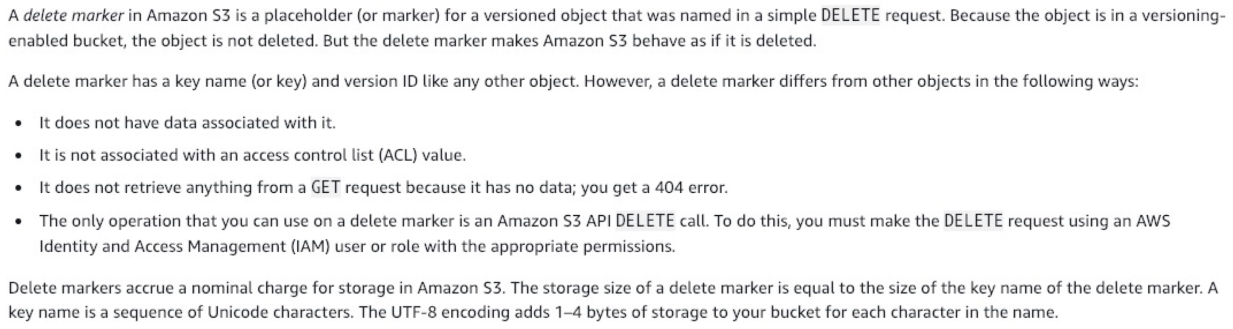
Explanation

Correct options:

A delete marker is set on the deleted object, but the actual object is not deleted - A delete marker in Amazon S3 is a placeholder (or marker) for a versioned object that was named in a simple DELETE request. Because the object is in a versioning-enabled bucket, the object is not deleted. But the delete marker makes Amazon S3 behave as if it is deleted. A delete marker has a key name (or key) and version ID like any other object. It does not have data associated with it. It is not associated with an access control list (ACL) value.

GET requests do not retrieve delete marker objects - The only way to list delete markers (and other versions of an object) is by using the versions subresource in a GET Bucket versions request. A simple GET does not retrieve delete marker objects.

What Delete Markers are:



A *delete marker* in Amazon S3 is a placeholder (or marker) for a versioned object that was named in a simple DELETE request. Because the object is in a versioning-enabled bucket, the object is not deleted. But the delete marker makes Amazon S3 behave as if it is deleted.

A delete marker has a key name (or key) and version ID like any other object. However, a delete marker differs from other objects in the following ways:

- It does not have data associated with it.
- It is not associated with an access control list (ACL) value.
- It does not retrieve anything from a GET request because it has no data; you get a 404 error.
- The only operation that you can use on a delete marker is an Amazon S3 API DELETE call. To do this, you must make the DELETE request using an AWS Identity and Access Management (IAM) user or role with the appropriate permissions.

Delete markers accrue a nominal charge for storage in Amazon S3. The storage size of a delete marker is equal to the size of the key name of the delete marker. A key name is a sequence of Unicode characters. The UTF-8 encoding adds 1–4 bytes of storage to your bucket for each character in the name.

via - https://docs.aws.amazon.com/AmazonS3/latest/userguide/DeleteMarker.html

Incorrect options:

GET requests can retrieve delete marker objects

A delete marker has a key, version ID and Access Control List (ACL) associated with it

The delete marker has the same data associated with it, as the actual object

These three options contradict the explanation provided above, so these options are incorrect.

Reference:

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

Question 33: **Correct**

A startup is looking at moving their web application to AWS Cloud. The database will be on Amazon RDS and it should not be accessible to the public. The application needs to remain connected to the database for the application to work. Also, the RDS instance will need access to the internet to download patches every month.

As a SysOps Administrator, how will you configure a solution for this requirement?

○ **Host the application servers in the public subnet of the VPC and database in the private subnet. The public subnet will connect to the internet using an Internet Gateway configured with the VPC. Database in the private subnet will use Network Address Translation (NAT) gateway, present in the** **(Correct)** public subnet, to connect to internet

○ Host the application servers in the public subnet and database in the private subnet of the VPC. The public subnet will connect to the internet using an Internet Gateway configured with the VPC. Use VPC-peering between the private and public subnets to open internet access for the database in private subnet

○ Host the application servers in the public subnet and database in the private subnet of the VPC. The public subnet will connect to the internet using an Internet Gateway configured with the VPC. The private subnet can connect to the internet if they are configured using IPv6 protocol

○ Host the application servers in the public subnet and database in the private subnet of the VPC. Configure Network Address Translation (NAT) gateway to provide access to the internet for both the subnets. The route table of both the subnets will have an entry to NAT gateway

Explanation

Correct option:

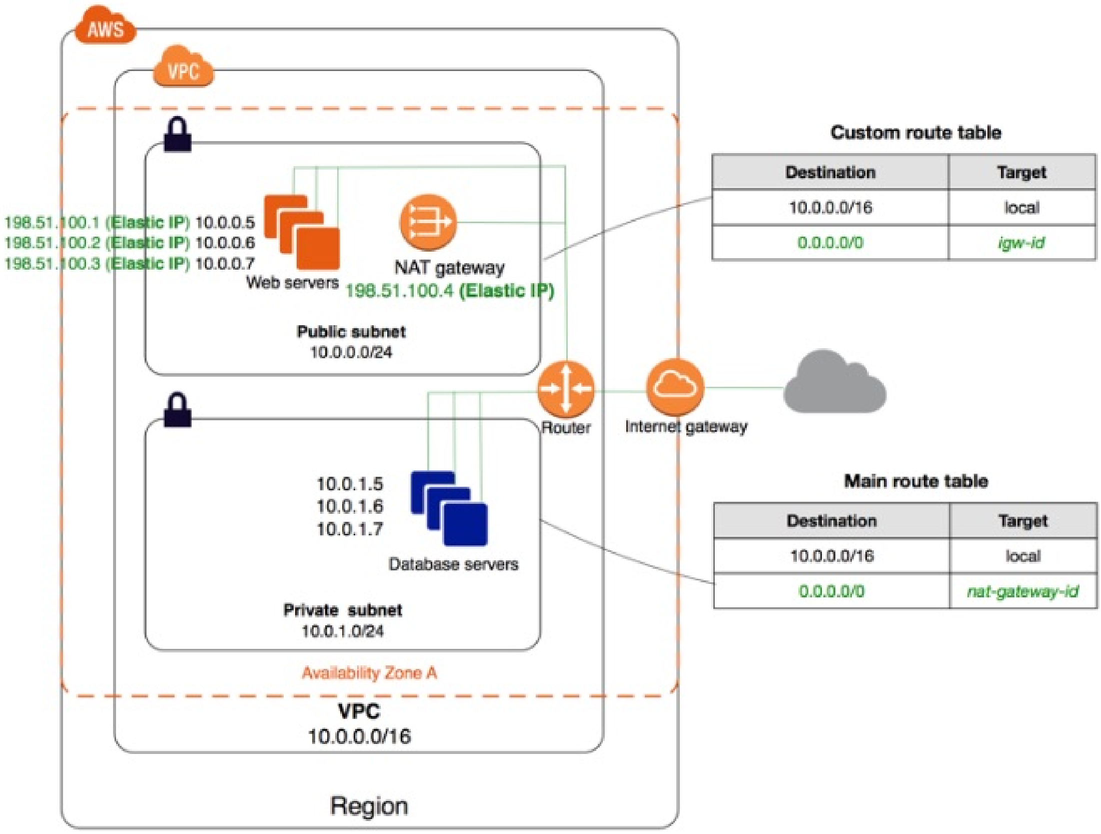
Host the application servers in the public subnet of the VPC and database in the private subnet. The public subnet will connect to the internet using an Internet Gateway configured with the VPC. Database in the private subnet will use Network Address Translation (NAT) gateway, present in the public subnet, to connect to internet

For a multi-tier website, with the application servers in a public subnet and the database servers in a private subnet, you can set up security and routing so that the application servers can communicate with the database servers.

The instances in the public subnet can send outbound traffic directly to the Internet, whereas the instances in the private subnet can't. Instead, the instances in the private subnet can access the Internet by using a network address translation (NAT) gateway that resides in the public subnet. The database servers can connect to the Internet for software updates using the NAT gateway, but the Internet cannot establish connections to the database servers.

Diagramatic representation of the above solution:

The following diagram shows the key components of the configuration for this scenario.



Custom route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*igw-id*

Main route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*nat-gateway-id*

via - https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html

Incorrect options:

Host the application servers in the public subnet and database in the private subnet of the VPC. Configure Network Address Translation (NAT) gateway to provide access to the internet for both the subnets. The route table of both the subnets will

have an entry to NAT gateway - NAT gateway is needed for instances in the private subnet to connect to the internet. NAT gateway is not used in public subnets, that have access to Internet Gateway.

Host the application servers in the public subnet and database in the private subnet of the VPC. The public subnet will connect to the internet using an Internet Gateway configured with the VPC. Use VPC-peering between the private and public subnets to open internet access for the database in private subnet - A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. It is a communication channel between VPCs, not between subnets of a VPC.

Host the application servers in the public subnet and database in the private subnet of the VPC. The public subnet will connect to the internet using an Internet Gateway configured with the VPC. The private subnet can connect to the internet if they are configured using IPv6 protocol - IPv6, like IPV4 is an internet protocol, used for communication over the internet. IPV6 does not provide internet access, if your instances use IPV6 for communication, you need to configure egress-only Internet gateway to connect to the internet.

Reference:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html

Question 34: **Correct**

A junior administrator at a retail company is documenting the process flow to provision EC2 instances via the Amazon EC2 API. These instances are to be used for an internal application that processes HR payroll data. He wants to highlight those volume types that cannot be used as a boot volume.

Can you help the intern by identifying those storage volume types that CANNOT be used as boot volumes while creating the instances? (Select two)

Cold HDD (sc1) **(Correct)**

□ **General Purpose SSD (gp2)**

□ **Instance Store**

□ **Throughput Optimized HDD (st1)** **(Correct)**

□ **Provisioned IOPS SSD (io1)**

Explanation

Correct options:

Throughput Optimized HDD (st1)

Cold HDD (sc1)

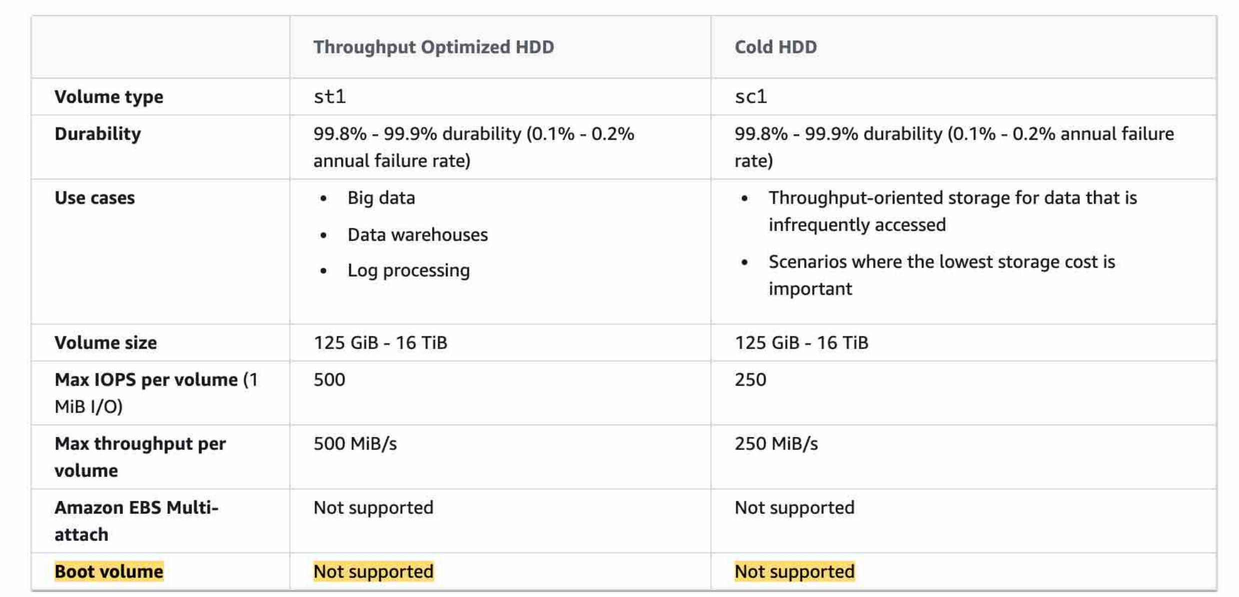
The EBS volume types fall into two categories:

SSD-backed volumes optimized for transactional workloads involving frequent read/write operations with small I/O size, where the dominant performance attribute is IOPS.

HDD-backed volumes optimized for large streaming workloads where throughput (measured in MiB/s) is a better performance measure than IOPS.

Throughput Optimized HDD (st1) and Cold HDD (sc1) volume types CANNOT be used as a boot volume, so these two options are correct.

Please see this detailed overview of the volume types for EBS volumes.



	Throughput Optimized HDD	Cold HDD
Volume type	`st1`	`sc1`
Durability	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)
Use cases	• Big data • Data warehouses • Log processing	• Throughput-oriented storage for data that is infrequently accessed • Scenarios where the lowest storage cost is important
Volume size	125 GiB - 16 TiB	125 GiB - 16 TiB
Max IOPS per volume (1 MiB I/O)	500	250
Max throughput per volume	500 MiB/s	250 MiB/s
Amazon EBS Multi-attach	Not supported	Not supported
Boot volume	Not supported	Not supported

via - https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html

Incorrect options:

General Purpose SSD (gp2)

Provisioned IOPS SSD (io1)

Instance Store

General Purpose SSD (gp2), Provisioned IOPS SSD (io1), and Instance Store can be used as a boot volume.

References:

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

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/RootDeviceStorage.html

Question 35: **Correct**

A retail company has a web application that is deployed on 10 EC2 instances running behind an Application Load Balancer. You have configured your web application to capture the IP address of the client making requests. When viewing the data captured you notice that every IP address being captured is the same, which also happens to be the IP address of the Application Load Balancer.

As a SysOps Administrator, what should you do to identify the true IP address of the client?

○ **Modify the front-end of the website so that the users send their IP in the requests**

○ **Look at the X-Forwarded-Proto header**

○ **Look at the X-Forwarded-For header** **(Correct)**

○ **Look at the client's cookie**

Explanation

Correct option:

Look at the X-Forwarded-For header

The X-Forwarded-For request header helps you identify the IP address of a client when you use an HTTP or HTTPS load balancer. Because load balancers intercept traffic between clients and servers, your server access logs contain only the IP address of the load balancer. To see the IP address of the client, use the X-Forwarded-For request header. Elastic Load Balancing stores the IP address of the client in the X-Forwarded-For request header and passes the header to your server.

Incorrect options:

Modify the front-end of the website so that the users send their IP in the requests - When a user makes a request the IP address is sent with the request to the server and the load balancer intercepts it. There is no need to modify the application.

Look at the X-Forwarded-Proto header - The X-Forwarded-Proto request header helps you identify the protocol (HTTP or HTTPS) that a client used to connect to your load balancer.

Look at the client's cookie - For this, we would need to modify the client-side logic and server-side logic, which would not be efficient.

Reference:

https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/x-forwarded-headers.html

Question 36: **Correct**

A data analytics company wants to seamlessly integrate its on-premises data center with AWS cloud-based IT systems which would be critical to manage as well as scale-up the complex planning and execution of every stage of its analytics workflows. As part of a pilot program, the company wants to integrate data files from its on-premises servers into AWS via an NFS interface.

Which of the following AWS service is the MOST efficient solution for the given use-case?

○ **AWS Storage Gateway - Tape Gateway**

○ **AWS Site-to-Site VPN**

○ **AWS Storage Gateway - Volume Gateway**

○ **AWS Storage Gateway - File Gateway** **(Correct)**

Explanation

Correct option:

AWS Storage Gateway - File Gateway

AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. The service provides three different types of gateways – Tape Gateway, File Gateway, and Volume Gateway – that seamlessly connect on-premises applications to cloud storage, caching data locally for low-latency access.

AWS Storage Gateway's file interface, or file gateway, offers you a seamless way to connect to the cloud in order to store application data files and backup images as durable objects on Amazon S3 cloud storage. File gateway offers SMB or NFS-based access to data in Amazon S3 with local caching. As the company wants to integrate data files from its analytical instruments into AWS via an NFS interface, therefore AWS Storage Gateway - File Gateway is the correct answer.

File Gateway Overview: via - https://docs.aws.amazon.com/storagegateway/latest/userguide/StorageGatewayConcepts.html

Incorrect options:

AWS Storage Gateway - Volume Gateway - You can configure the AWS Storage Gateway service as a Volume Gateway to present cloud-based iSCSI block storage volumes to your on-premises applications. Volume Gateway does not support NFS interface, so this option is not correct.

AWS Storage Gateway - Tape Gateway - AWS Storage Gateway - Tape Gateway allows moving tape backups to the cloud. Tape Gateway does not support NFS interface, so this option is not correct.

AWS Site-to-Site VPN - AWS Site-to-Site VPN enables you to securely connect your on-premises network or branch office site to your Amazon Virtual Private Cloud (Amazon VPC). You can securely extend your data center or branch office network to the cloud with an AWS Site-to-Site VPN (Site-to-Site VPN) connection. It uses internet protocol security (IPSec) communications to create encrypted VPN tunnels between two locations. You cannot use AWS Site-to-Site VPN to integrate data files via the NFS interface, so this option is not correct.

References:

https://aws.amazon.com/storagegateway/

https://aws.amazon.com/storagegateway/volume/

https://aws.amazon.com/storagegateway/file/

https://aws.amazon.com/storagegateway/vtl/

Question 37: **Correct**

As a SysOps Administrator, you have been tasked to generate a report on all API calls made for Elastic Load Balancer from the AWS Management Console.

Which feature/service will you use to fetch this data?

○ **CloudTrail logs** **(Correct)**

○ **Load Balancer Access logs**

○ **CloudWatch metrics**

○ **Load Balancer Request tracing**

Explanation

Correct option:

CloudTrail logs - Elastic Load Balancing is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Elastic Load Balancing. CloudTrail captures all API calls for Elastic Load Balancing as events. The calls captured include calls from the AWS Management Console and code calls to the Elastic Load Balancing API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Elastic Load Balancing. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in Event history. Using the information collected by CloudTrail, you can determine the request that was made to Elastic Load Balancing, the IP address from which the request was made, who made the request, when it was made, and additional details.

Incorrect options:

CloudWatch metrics - You can use Amazon CloudWatch to retrieve statistics about data points for your load balancers and targets as an ordered set of time-series data, known as metrics. You can use these metrics to verify that your system is performing as expected.

Load Balancer Access logs - You can use access logs to capture detailed information about the requests made to your load balancer and store them as log files in Amazon S3. You can use these access logs to analyze traffic patterns and to troubleshoot issues with your targets.

Load Balancer Request tracing - You can use request tracing to track HTTP requests. The load balancer adds a header with a trace identifier to each request it receives.

Reference:

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

Question 38: **Correct**

A social media company manages over 100 c4.large instances in the us-west-1 region. The EC2 instances run complex algorithms. The systems administrator would like to track CPU utilization of the EC2 instances as frequently as every 10 seconds.

Which of the following represents the BEST solution for the given use-case?

○ **Open a support ticket with AWS**

○ **Simply get it from the CloudWatch Metrics**

○ **Enable EC2 detailed monitoring**

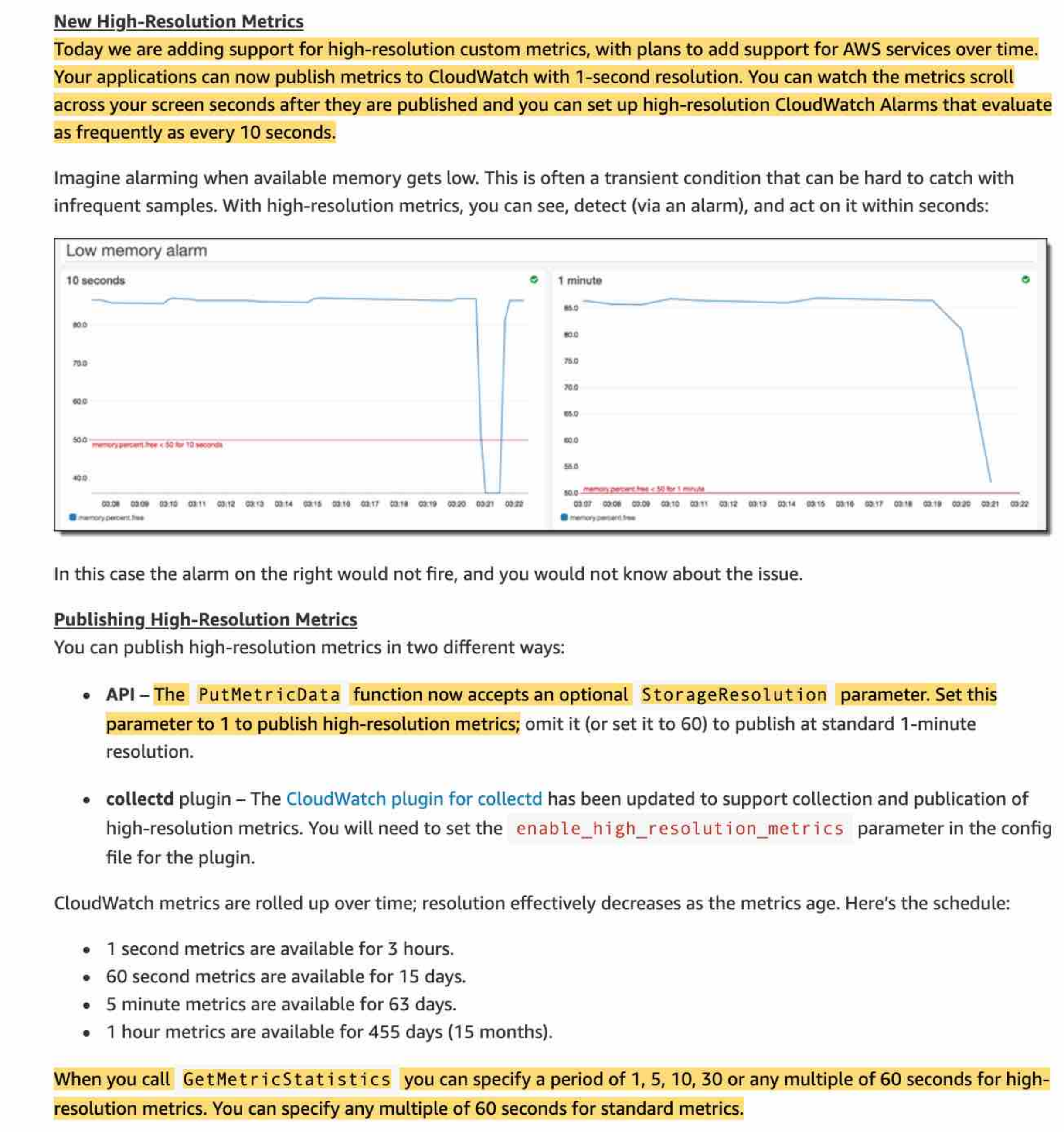
○ **Create a high-resolution custom metric and push the data using a script triggered every 10 seconds** **(Correct)**

Explanation

Correct option:

Create a high-resolution custom metric and push the data using a script triggered every 10 seconds

Using high-resolution custom metric, your applications can publish metrics to CloudWatch with 1-second resolution. You can watch the metrics scroll across your screen seconds after they are published and you can set up high-resolution CloudWatch Alarms that evaluate as frequently as every 10 seconds. You can alert with High-Resolution Alarms, as frequently as 10-second periods. High-Resolution Alarms allow you to react and take actions faster and support the same actions available today with standard 1-minute alarms.



New High-Resolution Metrics

Today we are adding support for high-resolution custom metrics, with plans to add support for AWS services over time. Your applications can now publish metrics to CloudWatch with 1-second resolution. You can watch the metrics scroll across your screen seconds after they are published and you can set up high-resolution CloudWatch Alarms that evaluate as frequently as every 10 seconds.

Imagine alarming when available memory gets low. This is often a transient condition that can be hard to catch with infrequent samples. With high-resolution metrics, you can see, detect (via an alarm), and act on it within seconds:

In this case the alarm on the right would not fire, and you would not know about the issue.

Publishing High-Resolution Metrics

You can publish high-resolution metrics in two different ways:

- **API** – The `PutMetricData` function now accepts an optional `StorageResolution` parameter. Set this parameter to 1 to publish high-resolution metrics; omit it (or set it to 60) to publish at standard 1-minute resolution.
- **collectd** plugin – The CloudWatch plugin for collectd has been updated to support collection and publication of high-resolution metrics. You will need to set the `enable_high_resolution_metrics` parameter in the config file for the plugin.

CloudWatch metrics are rolled up over time; resolution effectively decreases as the metrics age. Here's the schedule:

- 1 second metrics are available for 3 hours.
- 60 second metrics are available for 15 days.
- 5 minute metrics are available for 63 days.
- 1 hour metrics are available for 455 days (15 months).

When you call `GetMetricStatistics` you can specify a period of 1, 5, 10, 30 or any multiple of 60 seconds for high-resolution metrics. You can specify any multiple of 60 seconds for standard metrics.

via - https://aws.amazon.com/blogs/aws/new-high-resolution-custom-metrics-and-alarms-for-amazon-cloudwatch/

Incorrect options:

Enable EC2 detailed monitoring - As part of basic monitoring, Amazon EC2 sends metric data to CloudWatch in 5-minute periods. To send metric data for your instance to CloudWatch in 1-minute periods, you can enable detailed monitoring on the instance, however, this comes at an additional cost.

Simply get it from the CloudWatch Metrics - You can get data from metrics. The basic monitoring data is available automatically in a 5-minute interval and detailed monitoring data is available in a 1-minute interval.

Open a support ticket with AWS - This option has been added as a distractor.

Reference:

https://aws.amazon.com/blogs/aws/new-high-resolution-custom-metrics-and-alarms-for-amazon-cloudwatch/

Question 39: **Incorrect**

A banking service uses Amazon EC2 instances and Amazon RDS databases to run its core business functionalities. The Chief Technology Officer (CTO) of the company has requested granular OS level metrics from the database service for benchmarking.

As a SysOps Administrator, how will you provide this information?

○ **Subscribe to CloudWatch metrics that track CPU utilization of the instances the RDS is hosted on**

○ **Enable Enhanced Monitoring for your RDS DB instance** **(Correct)**

○ **Enable Performance Insights to expand on the existing Amazon RDS monitoring features to illustrate your database's performance** **(Incorrect)**

○ **Subscribe to Amazon RDS events to be notified when changes occur with a DB instance and its connected resources**

Explanation

Correct option:

Enable Enhanced Monitoring for your RDS DB instance - Amazon RDS provides metrics in real time for the operating system (OS) that your DB instance runs on. You can view the metrics for your DB instance using the console. Also, you can consume the Enhanced Monitoring JSON output from Amazon CloudWatch Logs in a monitoring system of your choice.

By default, Enhanced Monitoring metrics are stored for 30 days in the CloudWatch Logs, which are different from typical CloudWatch metrics. Enhanced Monitoring for RDS provides the following OS metrics: 1.Free Memory 2.Active Memory 3.Swap Free 4.Processes Running 5.File System Used

You can use these metrics to understand the environment's performance, and these metrics are ingested by Amazon CloudWatch Logs as log entries. You can use CloudWatch to create alarms based on metrics. These alarms run actions, and you can publish these metrics from within your infrastructure, device, or application into CloudWatch as a custom metric. By using Enhanced Monitoring and CloudWatch together, you can automate tasks by creating a custom metric for the CloudWatch Logs RDS ingested date from the Enhanced Monitoring metrics. Enhanced Monitoring metrics are useful when you want to see how different processes or threads on a DB instance use the CPU.

Incorrect options:

Subscribe to Amazon RDS events to be notified when changes occur with a DB instance and its connected resources - Subscribe to Amazon RDS events to be notified when changes occur with a DB instance, DB snapshot, DB parameter group, or DB security group. Amazon RDS uses the Amazon Simple Notification Service (Amazon SNS) to provide notification when an Amazon RDS event occurs. This option is not relevant for the given use-case.

Subscribe to CloudWatch metrics that track CPU utilization of the instances the RDS is hosted on - CloudWatch gathers metrics about CPU utilization from the hypervisor for a DB instance, and Enhanced Monitoring gathers its metrics from an agent on the instance. As a result, you might find differences between the measurements, because the hypervisor layer performs a small amount of work. The differences can be greater if your DB instances use smaller instance classes because then there are likely more virtual machines (VMs) that are managed by the hypervisor layer on a single physical instance. Enhanced Monitoring metrics are useful when you want to see how different processes or threads on a DB instance use the CPU.

Enable Performance Insights to expand on the existing Amazon RDS monitoring features to illustrate your database's performance - Performance Insights collects metric data from the database engine to monitor the actual load on a database. Performance Insights will not help in gathering granular OS level metrics.

Reference:

https://aws.amazon.com/premiumsupport/knowledge-center/custom-cloudwatch-metrics-rds/

Question 40: **Incorrect**

A retail company runs its server infrastructure on a fleet of Amazon EC2 instances with Amazon RDS as the database service. For the high availability of the entire architecture, multi-AZ deployments have been chosen for the RDS instance. A new version of the database engine has been released by the vendor and the company wants to test the release with production data and configurations before upgrading the production instance.

How will you configure this requirement?

○ **Create a configuration similar to the one in production using CloudFormation templates. You can reuse these templates to create any number of instances whenever required** **(Incorrect)**

○ **Create a read replica of the RDS instance in production. Upgrade the read replica to the latest version and experiment with this instance**

○ **Create a DB snapshot of your existing DB instance and create a new instance from the restored snapshot. Initiate a version upgrade on this new instance and safely experiment with the instance** **(Correct)**

○ **Procure an instance which has the new version of the database engine. Take the snapshot of your existing database and**

restore the snapshot to this instance. Test on this instance

Explanation

Correct option:

Create a DB snapshot of your existing DB instance and create a new instance from the restored snapshot. Initiate a version upgrade on this new instance and safely experiment with the instance

You can trial test the new version before opting it for production systems. To do so, create a DB snapshot of your existing DB instance, restore from the DB snapshot to create a new DB instance, and then initiate a version upgrade for the new DB instance. You can then experiment safely on the upgraded copy of your DB instance before deciding whether or not to upgrade your original DB instance.

Incorrect options:

Create a configuration similar to the one in production using CloudFormation templates. You can reuse these templates to create any number of instances whenever required - CloudFormation templates help in creating resources with the same configuration multiple times, in multiple AWS accounts, if needed. The given use-case requires an exact copy of the existing production database to trial test and CloudFormation cannot help in this scenario.

Create a read replica of the RDS instance in production. Upgrade the read replica to the latest version and experiment with this instance

Procure an instance that has the new version of the database engine. Take the snapshot of your existing database and restore the snapshot to this instance. Test on this instance

These two options are incorrect because to trial test a production database, we need a running database, in the same status as the existing one. This running database instance will be upgraded and then tested thoroughly to know its viability for production. The read replica operates as a DB instance that allows just read-only connections. Applications can connect to a read replica just as they would to any DB instance. The order of activities should be exactly the way it will be in production, so the upgrade goes smoothly without any glitches when done on the live system.

Reference:

https://aws.amazon.com/rds/faqs/

Question 41: **Incorrect**

The development team at an IT company is looking at moving its web applications to Amazon EC2 instances. The team is weighing its options for EBS volumes and instance store-backed instances for these applications with varied workloads.

Which of the following would you identify as correct regarding instance store and EBS volumes? (Select three)

Data stored in the instance store is preserved when you stop or terminate your instance. However, data is lost when you hibernate the instance. Configure EBS volumes or have a backup plan to avoid using critical data to this behavior **(Incorrect)**

Snapshots of EBS volumes, stored on Amazon S3, can be accessed using Amazon S3 APIs

EBS snapshots only capture data that has been written to your Amazon EBS volume, which might exclude any data that has been locally cached by your application or operating system **(Correct)**

By default, data on a non-root EBS volume is preserved even if the instance is shutdown or terminated (Correct)

EBS encryption does not support boot volumes

Use separate Amazon EBS volumes for the operating system and your data, even though root volume persistence feature is available (Correct)

Explanation

Correct options:

Use separate Amazon EBS volumes for the operating system and your data, even though root volume persistence feature is available

As a best practice, AWS recommends the use of separate Amazon EBS volumes for the operating system and your data. This ensures that the volume with your data persists even after instance termination or any issues to the operating system.

EBS snapshots only capture data that has been written to your Amazon EBS volume, which might exclude any data that has been locally cached by your application or operating system

Snapshots only capture data that has been written to your Amazon EBS volume, which might exclude any data that has been locally cached by your application or OS. To ensure consistent snapshots on volumes attached to an instance, AWS recommends detaching the volume cleanly, issuing the snapshot command, and then reattaching the volume. For Amazon EBS volumes that serve as root devices, AWS recommends shutting down the machine to take a clean snapshot.

By default, data on a non-root EBS volume is preserved even if the instance is shutdown or terminated

By default, when you attach a non-root EBS volume to an instance, its DeleteOnTermination attribute is set to false. Therefore, the default is to preserve these volumes. After the instance terminates, you can take a snapshot of the preserved volume or attach it to another instance. You must delete a volume to avoid incurring further charges.

Incorrect options:

Data stored in the instance store is preserved when you stop or terminate your instance. However, data is lost when you hibernate the instance. Configure EBS volumes or have a backup plan to avoid using critical data to this behavior - Data stored in instance store is lost when you stop, hibernate or terminate the instance.

EBS encryption does not support boot volumes - EBS volumes used as root devices can be encrypted without any issue.

Snapshots of EBS volumes, stored on Amazon S3, can be accessed using Amazon S3 APIs - This is incorrect. Snapshots are only available through the Amazon EC2 API.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-best-practices.html

https://aws.amazon.com/ebs/faqs/

Question 42: **Incorrect**

A new systems administrator has joined a large healthcare services company recently. As part of his onboarding, the IT department is conducting a review of the checklist for tasks related to AWS Identity and Access Management.

Which best practices would you recommend? (Select two)?

□ **Grant maximum privileges to avoid assigning privileges again**

□ **Configure AWS CloudTrail to log all IAM actions** (Correct)

□ **Use user credentials to provide access specific permissions for Amazon EC2 instances** (Incorrect)

Enable MFA for privileged users (Correct)

Create a minimum number of accounts and share these account credentials among employees

Explanation

Correct options:

Enable MFA for privileged users - As per the AWS best practices, it is better to enable Multi Factor Authentication (MFA) for privileged users via an MFA-enabled mobile device or hardware MFA token.

Configure AWS CloudTrail to record all account activity - AWS recommends to turn on CloudTrail to log all IAM actions for monitoring and audit purposes.

Incorrect options:

Create a minimum number of accounts and share these account credentials among employees - AWS recommends that user account credentials should not be shared between users. So, this option is incorrect.

Grant maximum privileges to avoid assigning privileges again - AWS recommends granting the least privileges required to complete a certain job and avoid giving excessive privileges which can be misused. So, this option is incorrect.

Use user credentials to provide access specific permissions for Amazon EC2 instances - It is highly recommended to use roles to grant access permissions for EC2 instances working on different AWS services. So, this option is incorrect.

References:

https://aws.amazon.com/iam/

https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html https://aws.amazon.com/cloudtrail/faqs/

Question 43: **Incorrect**

A large IT company uses several AWS accounts for the different lines of business. Quite often, the systems administrator is faced with the problem of sharing Customer Master Keys (CMKs) across multiple AWS accounts for accessing AWS resources spread across these accounts.

How will you implement a solution to address this issue?

○ **AWS Owned CMK can be used across AWS accounts. Configure an AWS Owned CMK and use it across accounts that need to share the key material** **(Incorrect)**

○ **Declare a key policy for the CMK to give the external account permission to use the CMK. This key policy should be embedded with the first request of every transaction**

○ **The key policy for the CMK must give the external account (or users and roles in the external account) permission to use the CMK. IAM policies in the external account must delegate the key policy permissions to its users and roles** **(Correct)**

○ **Use AWS KMS service-linked roles to share access across AWS accounts**

Explanation

Correct option:

The key policy for the CMK must give the external account (or users and roles in the external account) permission to use the CMK. IAM policies in the external account must delegate the key policy permissions to its users and roles

You can allow IAM users or roles in one AWS account to use a customer master key (CMK) in a different AWS account. You can add these permissions when you create the CMK or change the permissions for an existing CMK.

To permit the usage of a CMK to users and roles in another account, you must use two different types of policies:

1. The key policy for the CMK must give the external account (or users and roles in the external account) permission to use the CMK. The key policy is in the account that owns the CMK.
2. IAM policies in the external account must delegate the key policy permissions to its users and roles. These policies are set in the external account and give permissions to users and roles in that account.

Incorrect options:

AWS Owned CMK can be used across AWS accounts. Configure an AWS Owned CMK and use it across accounts that need to share the key material - AWS owned CMKs are a collection of CMKs that an AWS service owns and manages for use in multiple AWS accounts. However, you cannot view, use, track, or audit them

Use AWS KMS service-linked roles to share access across AWS accounts - AWS Key Management Service uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to AWS KMS. The service-linked roles are defined by AWS KMS and include all the permissions that the service requires to call other AWS services on your behalf. You cannot use AWS KMS service-linked roles to share access across AWS accounts.

Declare a key policy for the CMK to give the external account permission to use the CMK. This key policy should be embedded with the first request of every transaction - Key policy can not be directly shared across accounts.