Top 21 AWS Exam Questions

1. You are planning to build a fleet of EBS-optimized EC2 instances for your new application. Due to security compliance, your organization wants you to encrypt root volume which is used to boot the instances. How can this be achieved?

A. Select Encryption option for the root EBS volume while launching EC2 instance.

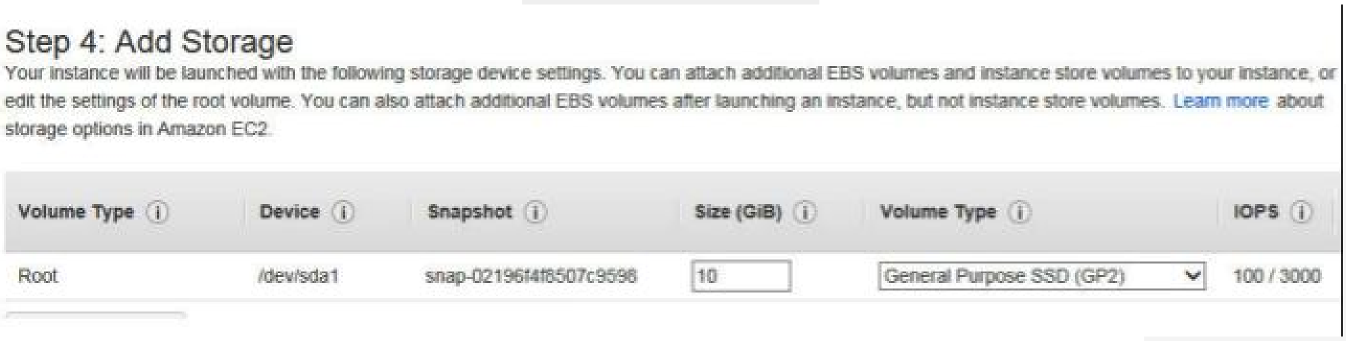
B. Once the EC2 instances are launched, encrypt the root volume using AWS KMS Master Key.

C. Root volumes cannot be encrypted. Add another EBS volume with encryption option selected during launch. Once EC2 instances are launched, make encrypted EBS volume as root volume through the console.

D. Launch an unencrypted EC2 instance and create a snapshot of the root volume. Make a copy of the snapshot with the encryption option selected and CreateImage using encrypted snapshot. Use this image to launch EC2 instances.

Answer: D

When launching an EC2 instance, the EBS volume for root cannot be encrypted.

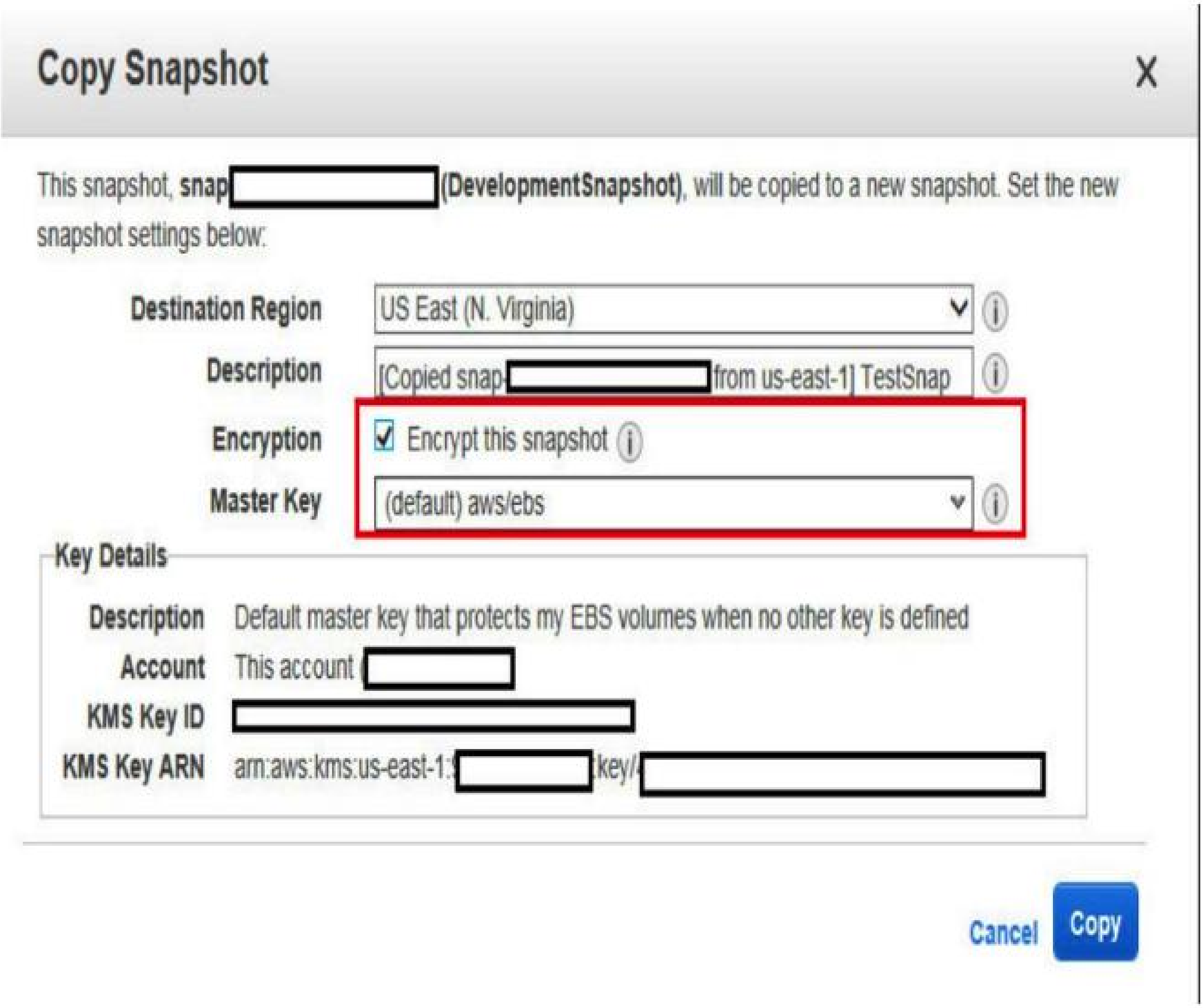


Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ
Root	/dev/sda1	snap-02196f4f8507c9598	10	General Purpose SSD (GP2)	100 / 3000

You can launch the instance with unencrypted root volume and create a snapshot of the root volume. Once the snapshot is created, you can copy the snapshot where you can make the new snapshot encrypted.



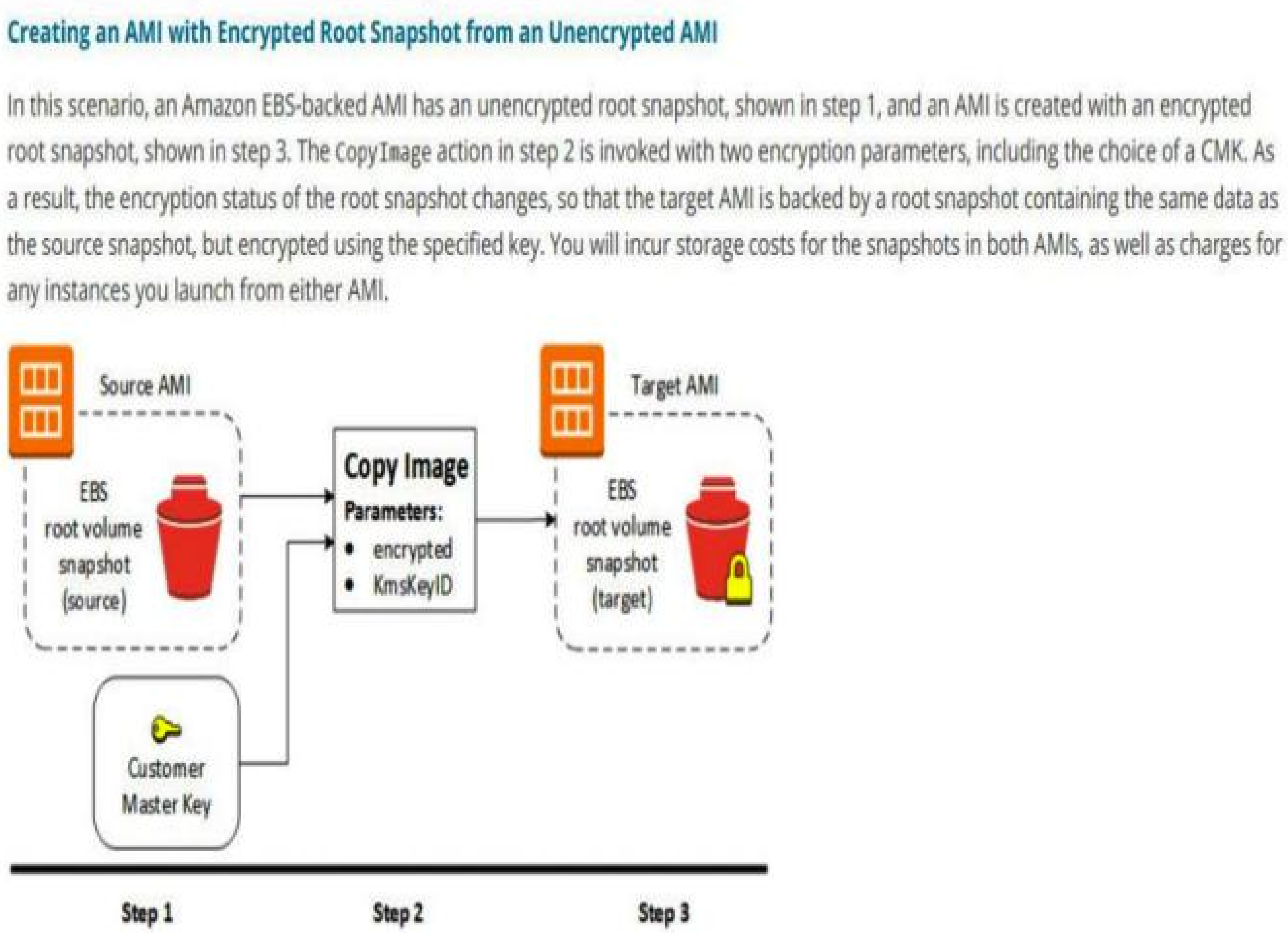
Copy Snapshot

This snapshot, **snap**[redacted]**(DevelopmentSnapshot)**, will be copied to a new snapshot. Set the new snapshot settings below:

Destination Region	US East (N. Virginia)
Description	[Copied snap[redacted]from us-east-1] TestSnap
Encryption	☑ Encrypt this snapshot
Master Key	(default) aws/ebs

Key Details

Description	Default master key that protects my EBS volumes when no other key is defined
Account	This account ([redacted]
KMS Key ID	[redacted]
KMS Key ARN	arn:aws:kms:us-east-1:[redacted]key/[redacted]



Creating an AMI with Encrypted Root Snapshot from an Unencrypted AMI

In this scenario, an Amazon EBS-backed AMI has an unencrypted root snapshot, shown in step 1, and an AMI is created with an encrypted root snapshot, shown in step 3. The `CopyImage` action in step 2 is invoked with two encryption parameters, including the choice of a CMK. As a result, the encryption status of the root snapshot changes, so that the target AMI is backed by a root snapshot containing the same data as the source snapshot, but encrypted using the specified key. You will incur storage costs for the snapshots in both AMIs, as well as charges for any instances you launch from either AMI.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIEncryption.html#AMIEncryption_

2. Organization XYZ is planning to build an online chat application for their enterprise level col laboration for their employees across the world. They are looking for a single digit latency fully managed database to store and retrieve conversations. What would AWS Database service you recommend?

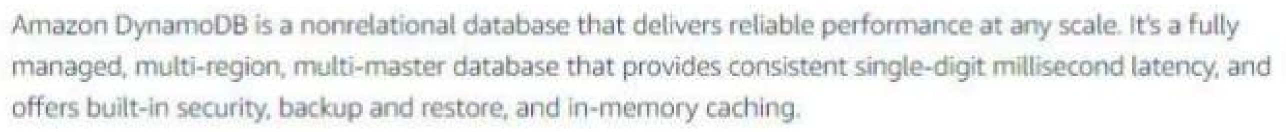
A. AWS DynamoDB

B. AWS RDS

C. AWS Redshift

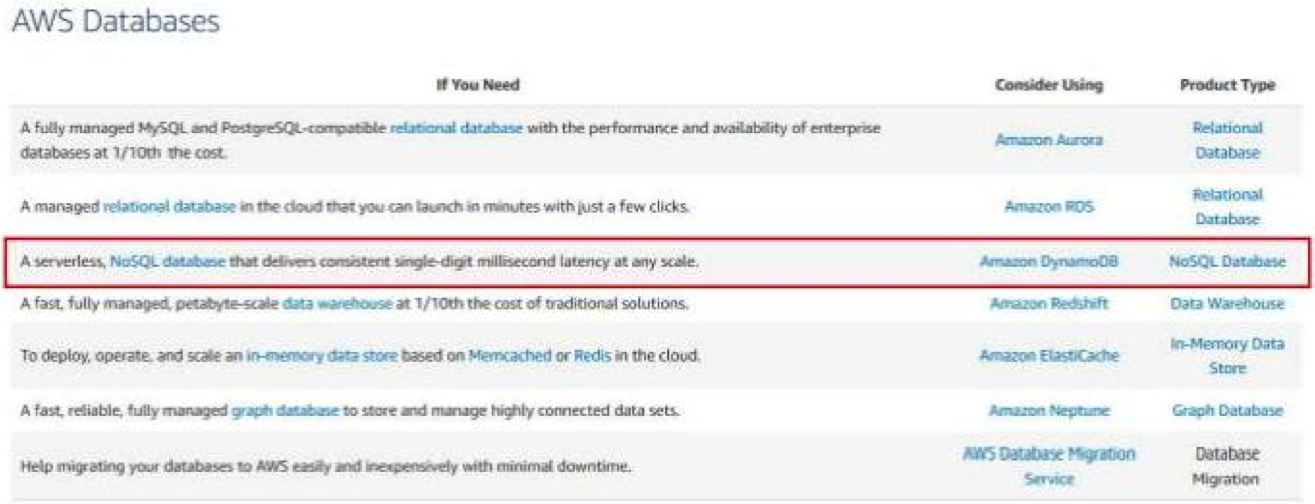
D. AWS Aurora

Answer: A



Amazon DynamoDB is a nonrelational database that delivers reliable performance at any scale. It's a fully managed, multi-region, multi-master database that provides consistent single-digit millisecond latency, and offers built-in security, backup and restore, and in-memory caching.

https://aws.amazon.com/dynamodb/#whentousedynamodb



AWS Databases

If You Need	Consider Using	Product Type
A fully managed MySQL and PostgreSQL-compatible relational database with the performance and availability of enterprise databases at 1/10th the cost.	Amazon Aurora	Relational Database
A managed relational database in the cloud that you can launch in minutes with just a few clicks.	Amazon RDS	Relational Database
A serverless, NoSQL database that delivers consistent single-digit millisecond latency at any scale.	Amazon DynamoDB	NoSQL Database
A fast, fully managed, petabyte-scale data warehouse at 1/10th the cost of traditional solutions.	Amazon Redshift	Data Warehouse
To deploy, operate, and scale an in-memory data store based on Memcached or Redis in the cloud.	Amazon ElastiCache	In-Memory Data Store
A fast, reliable, fully managed graph database to store and manage highly connected data sets.	Amazon Neptune	Graph Database
Help migrating your databases to AWS easily and inexpensively with minimal downtime.	AWS Database Migration Service	Database Migration

Try Now: AWS Certified Solutions Architect Associate Free Test

3. When creating an AWS CloudFront distribution, which of the following is not an origin?

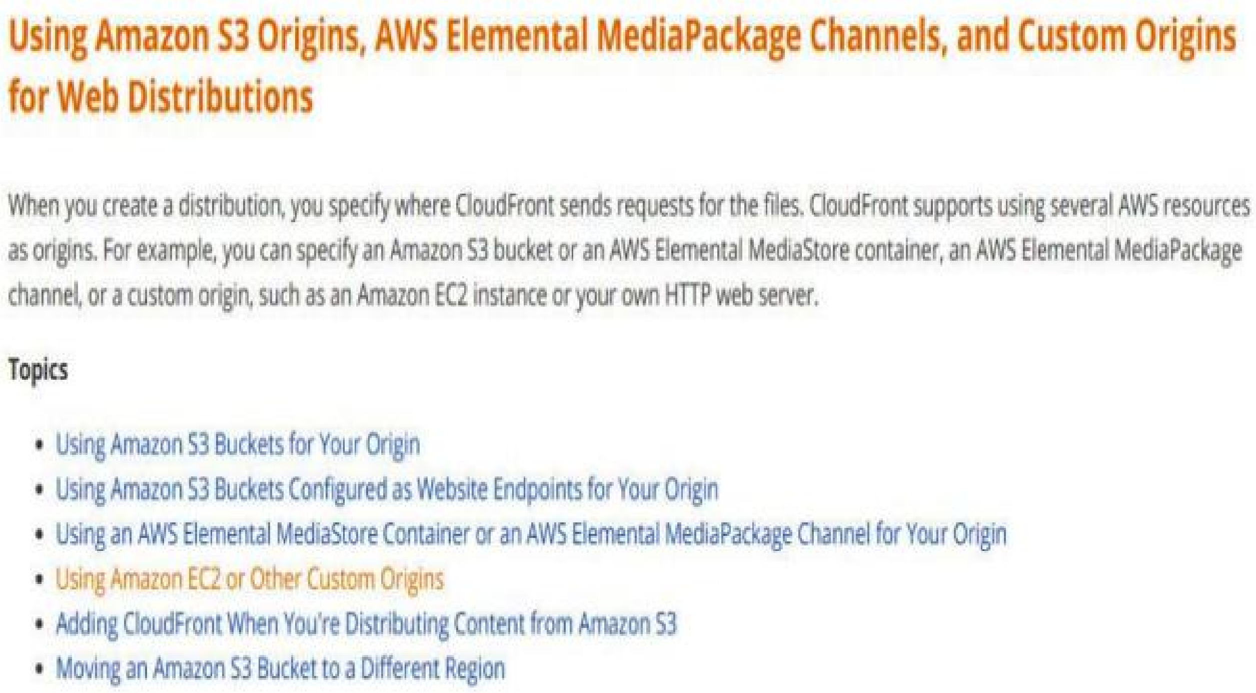
A. Elastic Load Balancer

B. AWS S3 bucket

C. AWS MediaPackage channel endpoint

D. AWS Lambda

Answer: D



Using Amazon S3 Origins, AWS Elemental MediaPackage Channels, and Custom Origins for Web Distributions

When you create a distribution, you specify where CloudFront sends requests for the files. CloudFront supports using several AWS resources as origins. For example, you can specify an Amazon S3 bucket or an AWS Elemental MediaStore container, an AWS Elemental MediaPackage channel, or a custom origin, such as an Amazon EC2 instance or your own HTTP web server.

Topics

- Using Amazon S3 Buckets for Your Origin
- Using Amazon S3 Buckets Configured as Website Endpoints for Your Origin
- Using an AWS Elemental MediaStore Container or an AWS Elemental MediaPackage Channel for Your Origin
- Using Amazon EC2 or Other Custom Origins
- Adding CloudFront When You're Distributing Content from Amazon S3
- Moving an Amazon S3 Bucket to a Different Region

Explanation: AWS Lambda is not supported directly as the CloudFront origin. However, Lambda can be invoked through API Gateway which can be set as the origin for AWS CloudFront.

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html

4. Which of the following statements are true with respect to VPC? (choose multiple)

A. A subnet can have multiple route tables associated with it.

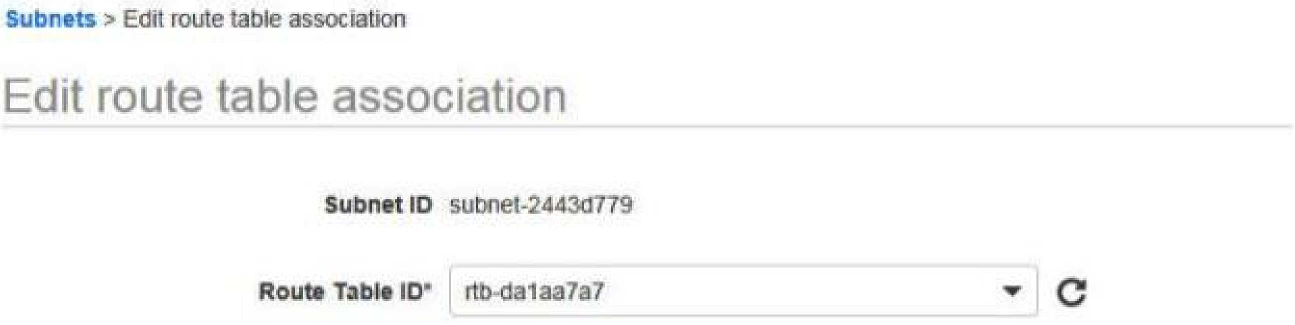
B. A network ACL can be associated with multiple subnets.

C. A route with target “local” on the route table can be edited to restrict traffic within VPC.

D. Subnet’s IP CIDR block can be same as the VPC CIDR block.

Answer: B, D

Option A is not correct. A subnet can have only one route table associated with it.



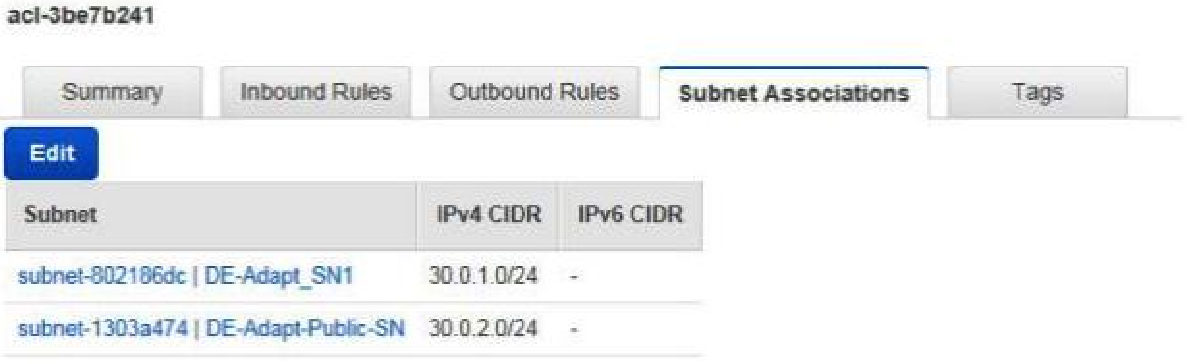
Subnets > Edit route table association

Edit route table association

Subnet ID subnet-2443d779

Route Table ID* rtb-da1aa7a7

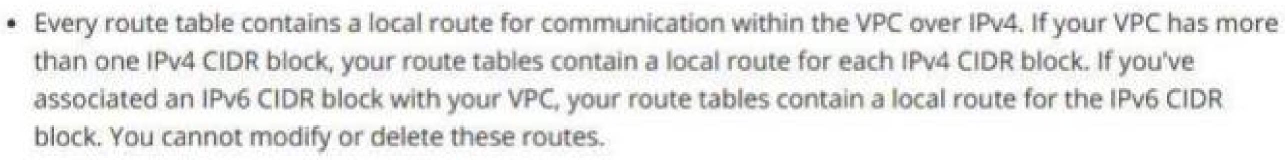
Option B is correct.



acl-3be7b241

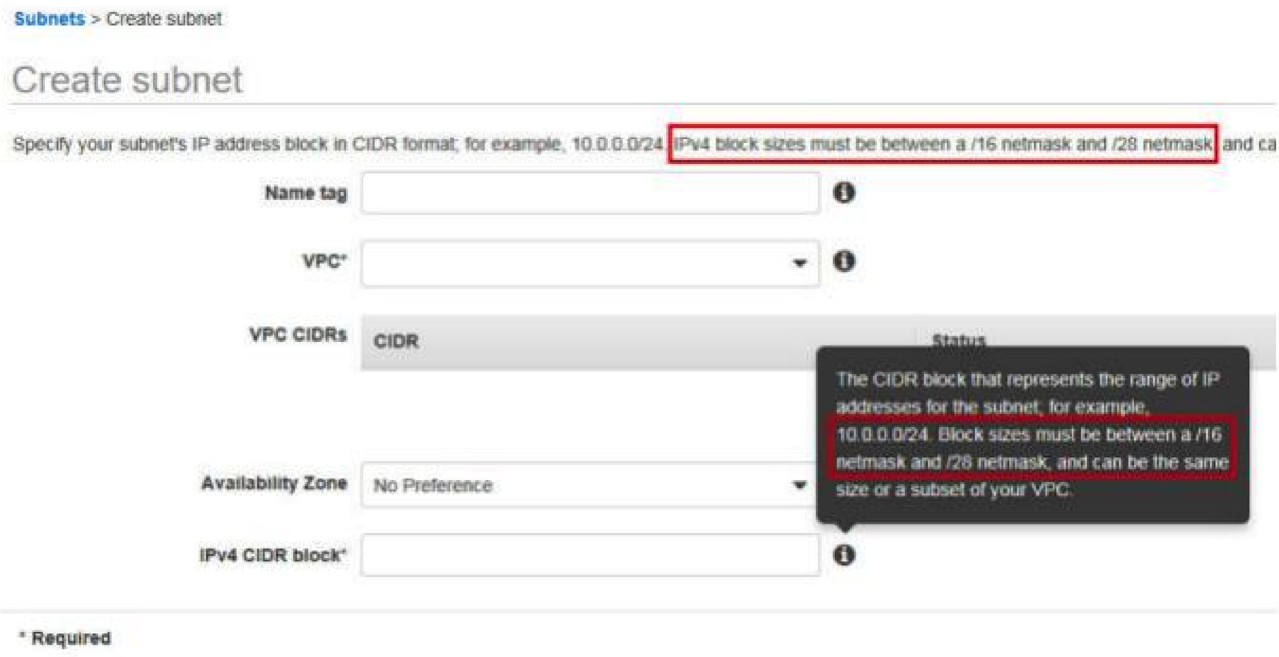
Subnet	IPv4 CIDR	IPv6 CIDR
subnet-802186dc | DE-Adapt_SN1	30.0.1.0/24	-
subnet-1303a474 | DE-Adapt-Public-SN	30.0.2.0/24	-

Option C is not correct.



- Every route table contains a local route for communication within the VPC over IPv4. If your VPC has more than one IPv4 CIDR block, your route tables contain a local route for each IPv4 CIDR block. If you've associated an IPv6 CIDR block with your VPC, your route tables contain a local route for the IPv6 CIDR block. You cannot modify or delete these routes.

Option D is correct.



Subnets > Create subnet

Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask and ca

Name tag

VPC*

VPC CIDRs

CIDR	Status

Availability Zone: No Preference

IPv4 CIDR block*

The CIDR block that represents the range of IP addresses for the subnet; for example, 10.0.0.0/24. Block sizes must be between a /16 netmask and /28 netmask, and can be the same size or a subset of your VPC.

* Required

5. Organization ABC has a customer base in US and Australia that would be downloading 10s of GBs files from your application. For them to have a better download experience, they decided to use AWS S3 bucket with cross-region replication with the US as source and Australia as the destination. They are using existing unused S3 buckets and had setup cross-region replication successfully. However, when files uploaded to US bucket, they are not being replicated to Australia bucket. What could be the reason?

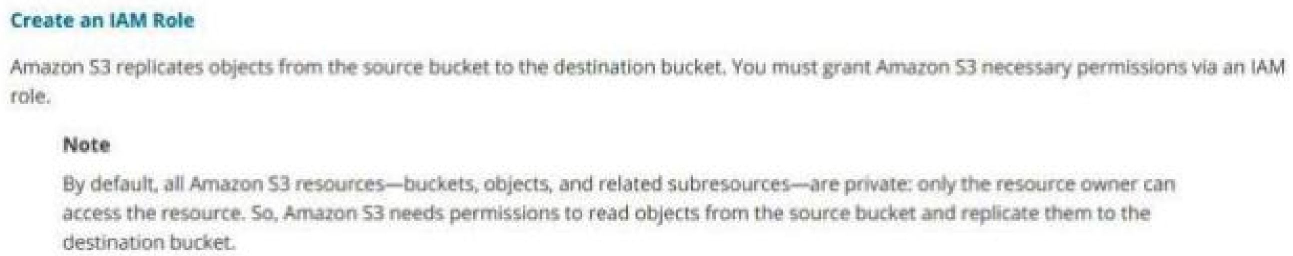
A. Versioning is not enabled on the source and destination buckets.

B. Encryption is not enabled on the source and destination buckets.

C. Source bucket has a policy with DENY and role used for replication is not excluded from DENY.

D. Destination bucket's default CORS policy does not have source bucket added as the origin.

Answer: C



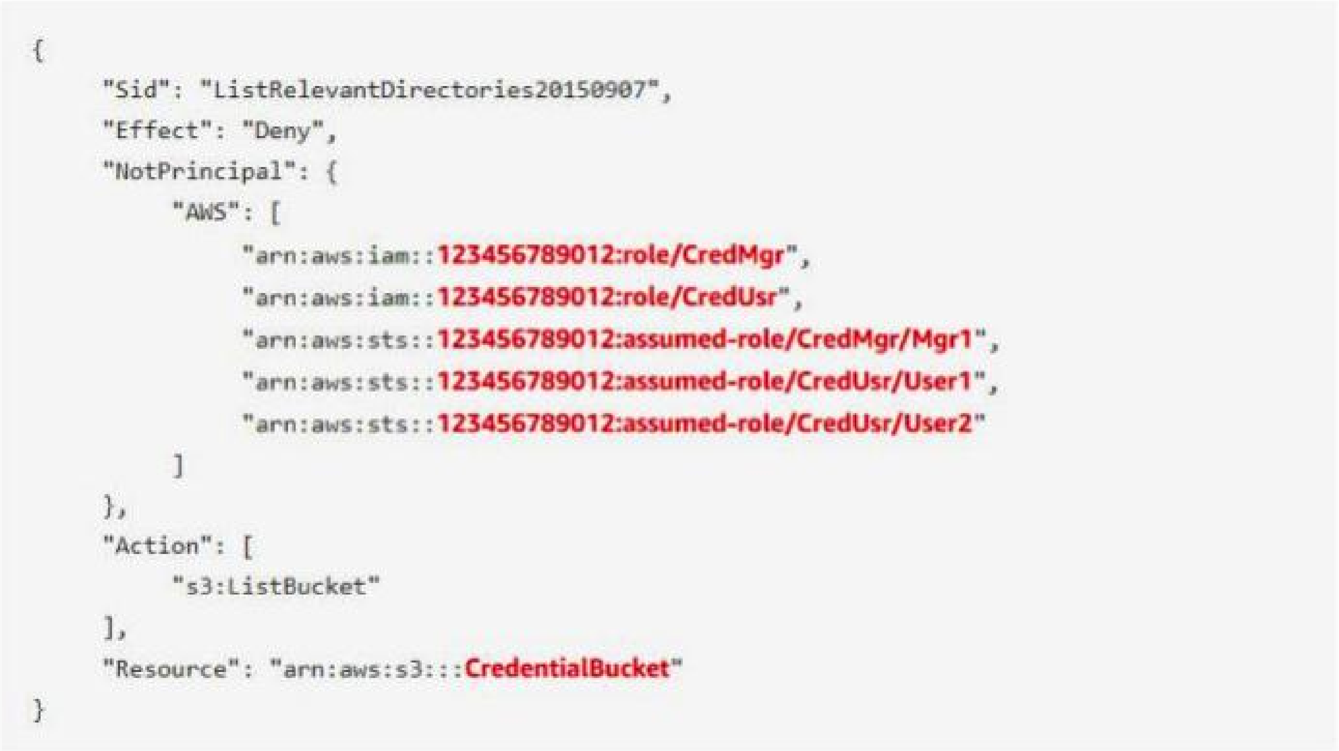
Create an IAM Role

Amazon S3 replicates objects from the source bucket to the destination bucket. You must grant Amazon S3 necessary permissions via an IAM role.

Note

By default, all Amazon S3 resources—buckets, objects, and related subresources—are private: only the resource owner can access the resource. So, Amazon S3 needs permissions to read objects from the source bucket and replicate them to the destination bucket.

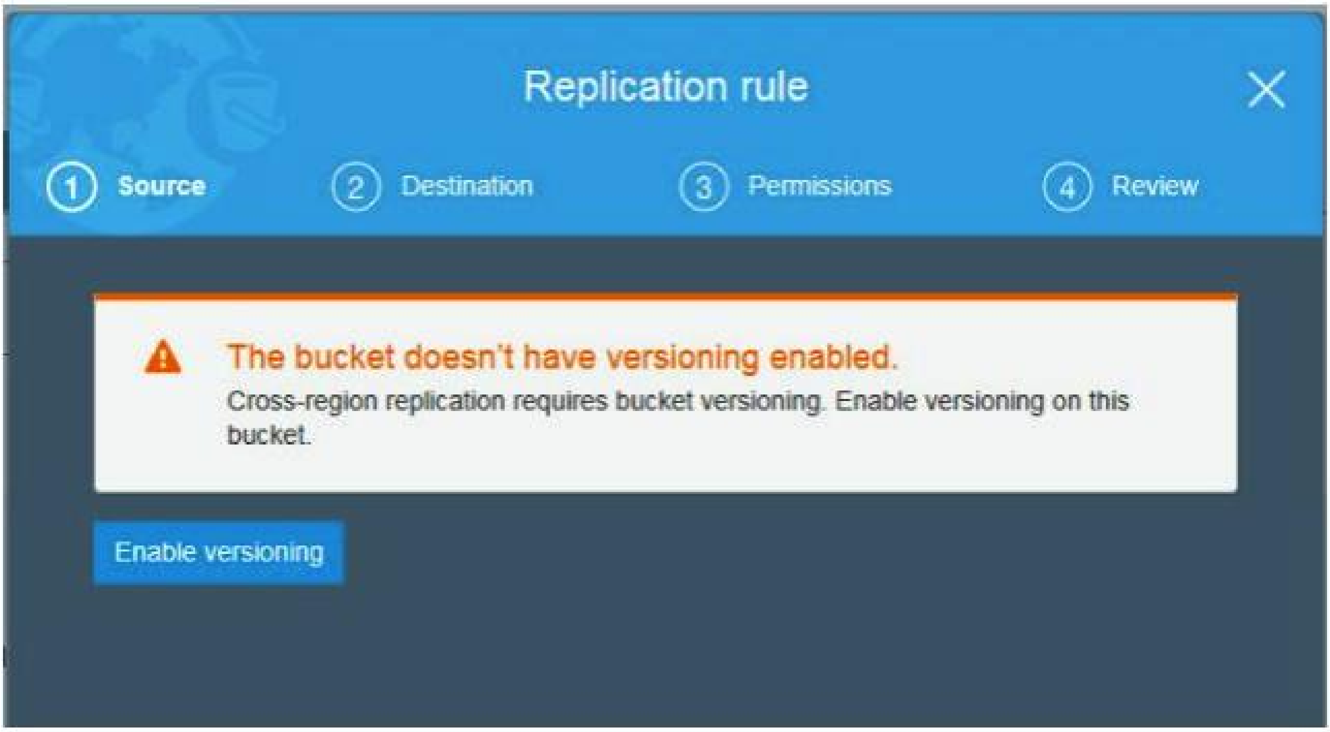
When you have a bucket policy which has explicit DENY, you must exclude all IAM resources which need to access the bucket.



```
{
     "Sid": "ListRelevantDirectories20150907",
     "Effect": "Deny",
     "NotPrincipal": {
          "AWS": [
               "arn:aws:iam::123456789012:role/CredMgr",
               "arn:aws:iam::123456789012:role/CredUsr",
               "arn:aws:sts::123456789012:assumed-role/CredMgr/Mgr1",
               "arn:aws:sts::123456789012:assumed-role/CredUsr/User1",
               "arn:aws:sts::123456789012:assumed-role/CredUsr/User2"
          ]
     },
     "Action": [
          "s3:ListBucket"
     ],
     "Resource": "arn:aws:s3:::CredentialBucket"
}
```

https://aws.amazon.com/blogs/security/how-to-create-a-policy-that-whitelists-access-to-sensitive-amazon-s3-buckets/

For option A, Cross region replication cannot be enabled without enabling versioning. The question states that cross-region replication has been successfully enabled. So this option is not correct.



Replication rule

The bucket doesn't have versioning enabled.

Cross-region replication requires bucket versioning. Enable versioning on this bucket.

6. Which of the following is not a category in AWS Trusted Advisor service checks?

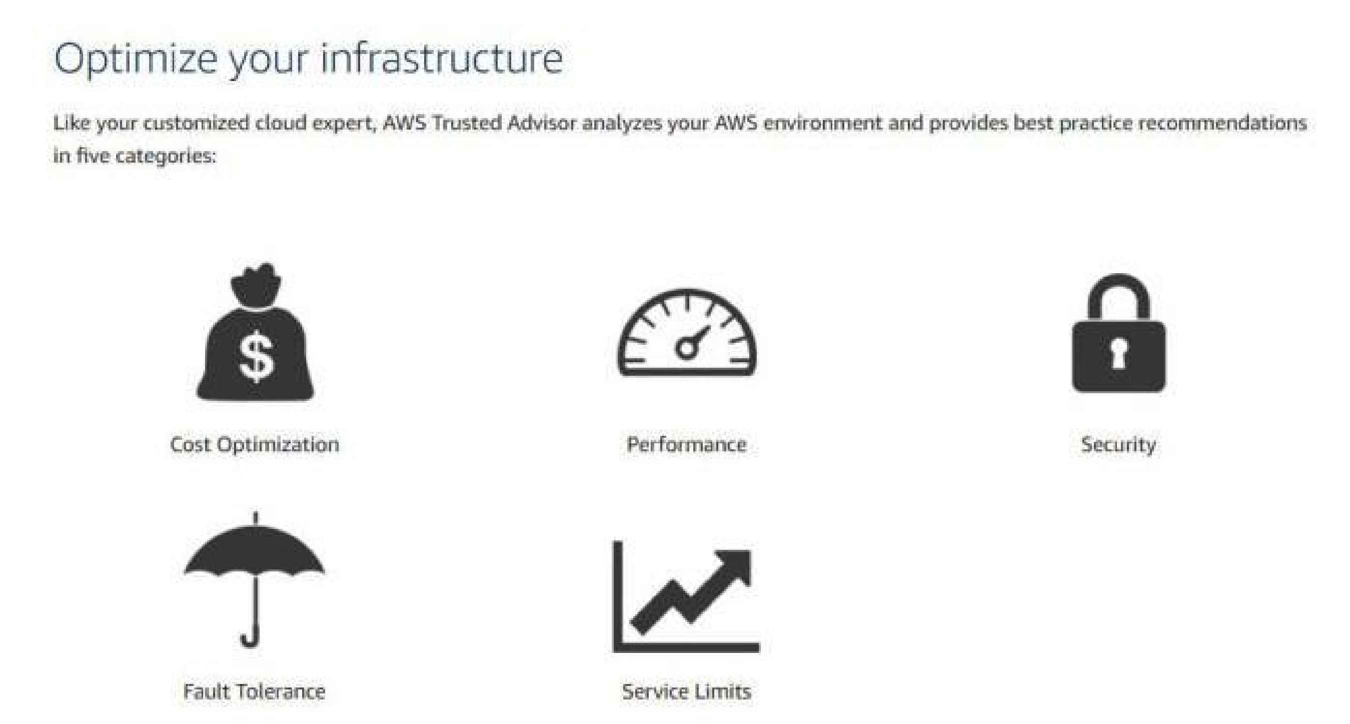
A. Cost Optimization

B. Fault Tolerance

C. Service Limits

D. Network Optimization

Answer: D



Optimize your infrastructure

Like your customized cloud expert, AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations in five categories:

https://aws.amazon.com/premiumsupport/technology/trusted-advisor/

7. Your organization is building a collaboration platform for which they chose AWS EC2 for web and application servers and MySQL RDS instance as the database. Due to the nature of the traffic to the application, they would like to increase the number of connections to RDS instance. How can this be achieved?

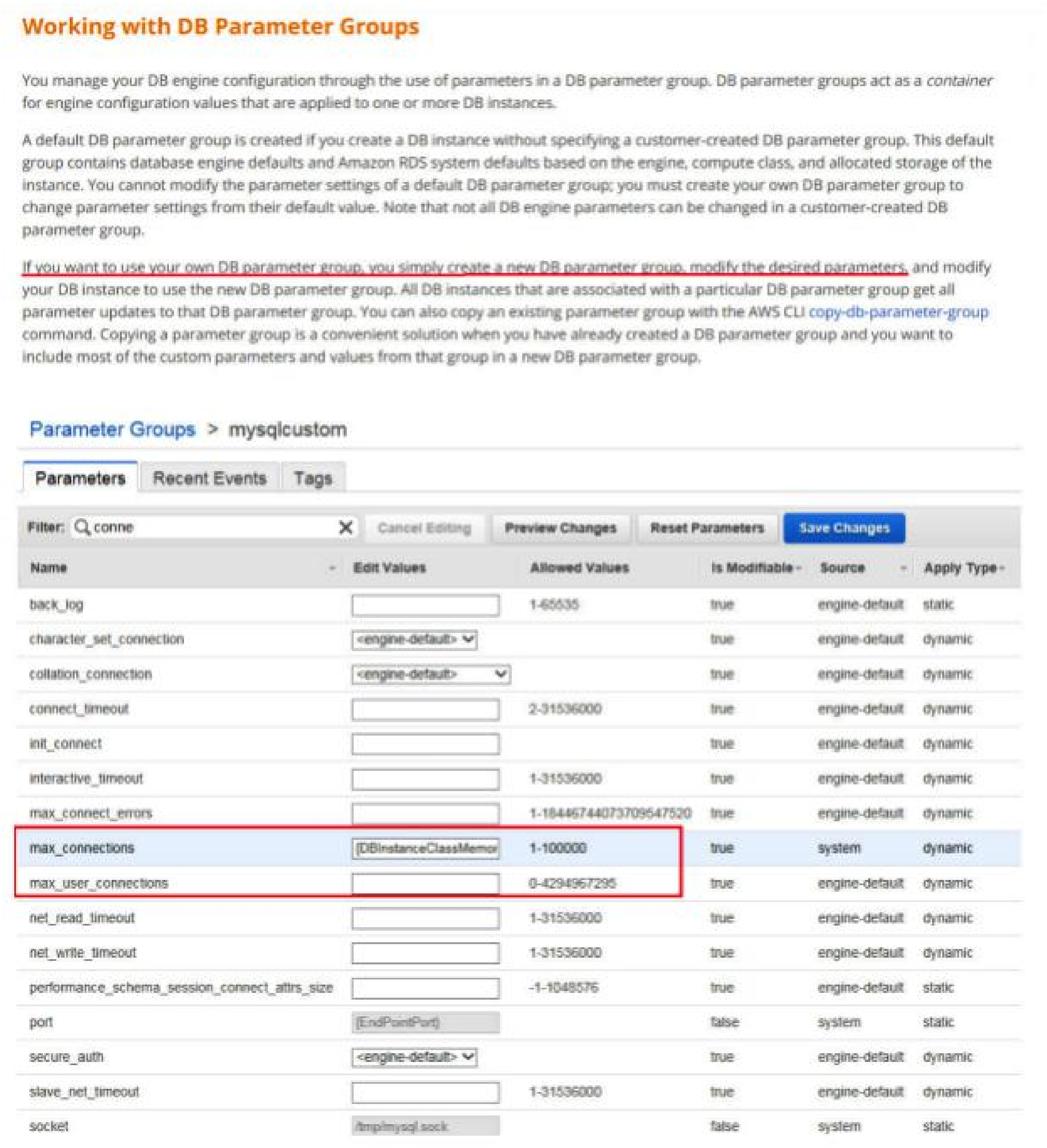
A. Login to RDS instance and modify database config file under /etc/mysql/my.cnf

B. Create a new parameter group, attach it to DB instance and change the setting.

C. Create a new option group, attach it to DB instance and change the setting.

D. Modify setting in default options group attached to DB instance.

Answer: B



Working with DB Parameter Groups

You manage your DB engine configuration through the use of parameters in a DB parameter group. DB parameter groups act as a *container* for engine configuration values that are applied to one or more DB instances.

A default DB parameter group is created if you create a DB instance without specifying a customer-created DB parameter group. This default group contains database engine defaults and Amazon RDS system defaults based on the engine, compute class, and allocated storage of the instance. You cannot modify the parameter settings of a default DB parameter group; you must create your own DB parameter group to change parameter settings from their default value. Note that not all DB engine parameters can be changed in a customer-created DB parameter group.

If you want to use your own DB parameter group, you simply create a new DB parameter group, modify the desired parameters, and modify your DB instance to use the new DB parameter group. All DB instances that are associated with a particular DB parameter group get all parameter updates to that DB parameter group. You can also copy an existing parameter group with the AWS CLI copy-db-parameter-group command. Copying a parameter group is a convenient solution when you have already created a DB parameter group and you want to include most of the custom parameters and values from that group in a new DB parameter group.

Parameter Groups > mysqlcustom

Name	Edit Values	Allowed Values	Is Modifiable	Source	Apply Type
back_log		1-65535	true	engine-default	static
character_set_connection	<engine-default>		true	engine-default	dynamic
collation_connection	<engine-default>		true	engine-default	dynamic
connect_timeout		2-31536000	true	engine-default	dynamic
init_connect			true	engine-default	dynamic
interactive_timeout		1-31536000	true	engine-default	dynamic
max_connect_errors		1-18446744073709547520	true	engine-default	dynamic
max_connections	{DBInstanceClassMemor	1-100000	true	system	dynamic
max_user_connections		0-4294967295	true	engine-default	dynamic
net_read_timeout		1-31536000	true	engine-default	dynamic
net_write_timeout		1-31536000	true	engine-default	dynamic
performance_schema_session_connect_attrs_size		-1-1048576	true	engine-default	static
port	{EndPointPort}		false	system	static
secure_auth	<engine-default>		true	engine-default	dynamic
slave_net_timeout		1-31536000	true	engine-default	dynamic
socket	/tmp/mysql.sock		false	system	static

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithParamGroups.html

8. You will be launching and terminating EC2 instances on need basis for your workloads. You need to run some shell scripts and perform certain checks connecting to AWS S3 bucket when the instance is getting launched. Which of the following options will allow performing any tasks during launch? (choose multiple)

A. Use Instance user data for shell scripts.

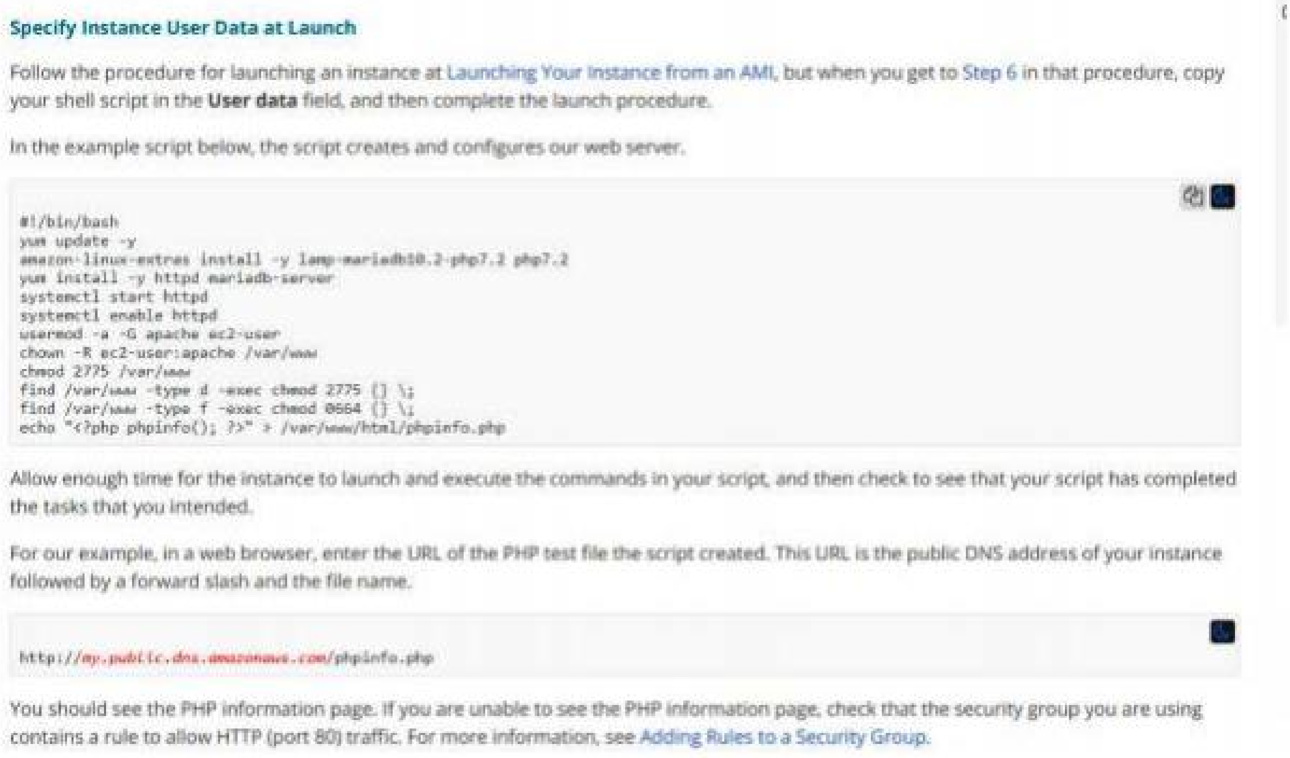
B. Use Instance metadata for shell scripts.

C. Use AutoScaling Group lifecycle hooks and trigger AWS Lambda function through Cloud Watch events.

D. Use Placement Groups and set “InstanceLaunch” state to trigger AWS Lambda functions.

Answer: A, C

Option A is correct.



Specify Instance User Data at Launch

Follow the procedure for launching an instance at Launching Your Instance from an AMI, but when you get to Step 6 in that procedure, copy your shell script in the **User data** field, and then complete the launch procedure.

In the example script below, the script creates and configures our web server.

```
#!/bin/bash
yum update -y
amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
yum install -y httpd mariadb-server
systemctl start httpd
systemctl enable httpd
usermod -a -G apache ec2-user
chown -R ec2-user:apache /var/www
chmod 2775 /var/www
find /var/www -type d -exec chmod 2775 {} \;
find /var/www -type f -exec chmod 0664 {} \;
echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
```

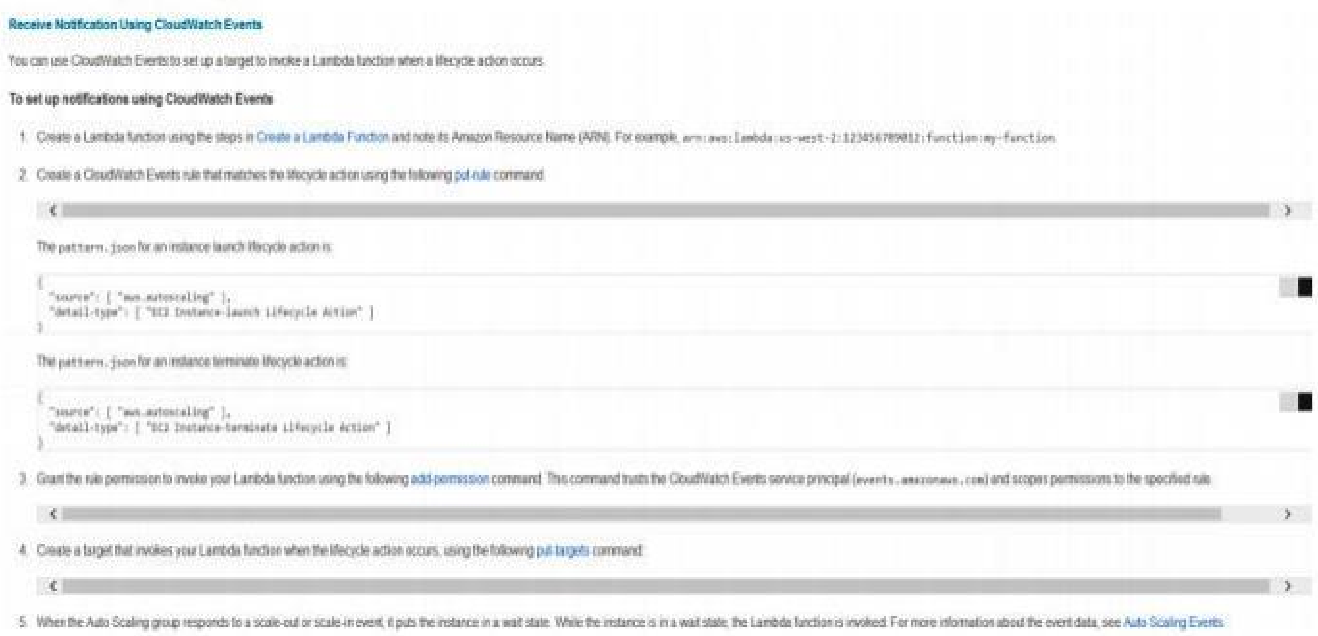
Allow enough time for the instance to launch and execute the commands in your script, and then check to see that your script has completed the tasks that you intended.

For our example, in a web browser, enter the URL of the PHP test file the script created. This URL is the public DNS address of your instance followed by a forward slash and the file name.

```
http://my.public.dns.amazonaws.com/phpinfo.php
```

You should see the PHP information page. If you are unable to see the PHP information page, check that the security group you are using contains a rule to allow HTTP (port 80) traffic. For more information, see Adding Rules to a Security Group.

Option C is correct.



Receive Notification Using CloudWatch Events

You can use CloudWatch Events to set up a target to invoke a Lambda function when a lifecycle action occurs.

To set up notifications using CloudWatch Events

1. Create a Lambda function using the steps in Create a Lambda Function and note its Amazon Resource Name (ARN). For example, `arn:aws:lambda:us-west-2:123456789012:function:my-function`
2. Create a CloudWatch Events rule that matches the lifecycle action using the following put-rule command.

   The `pattern.json` for an instance launch lifecycle action is:

```
{
  "source": [ "aws.autoscaling" ],
  "detail-type": [ "EC2 Instance-launch Lifecycle Action" ]
}
```

   The `pattern.json` for an instance terminate lifecycle action is:

```
{
  "source": [ "aws.autoscaling" ],
  "detail-type": [ "EC2 Instance-terminate Lifecycle Action" ]
}
```

3. Grant the rule permission to invoke your Lambda function using the following add-permission command. This command trusts the CloudWatch Events service principal (`events.amazonaws.com`) and scopes permissions to the specified rule.
4. Create a target that invokes your Lambda function when the lifecycle action occurs, using the following put-targets command.
5. When the Auto Scaling group responds to a scale-out or scale-in event, it puts the instance in a wait state. While the instance is in a wait state, the Lambda function is invoked. For more information about the event data, see Auto Scaling Events.

https://docs.aws.amazon.com/autoscaling/ec2/userguide/lifecycle-hooks.html#preparing-for-notification

9. Your organization has an AWS setup and planning to build Single Sign-On for users to authenticate with on-premise Microsoft Active Directory Federation Services (ADFS) and let users log in to AWS console using AWS STS Enterprise Identity Federation. Which of the following service do you need to call from AWS STS service after you authenticate with your on-premise?

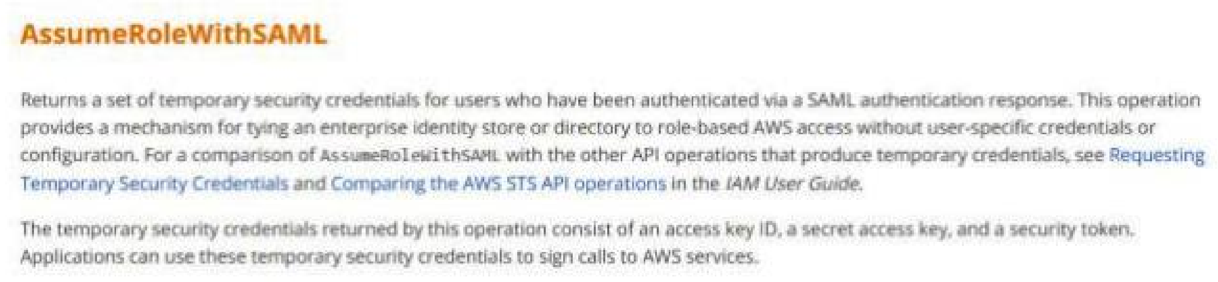
A. AssumeRoleWithSAML

B. GetFederationToken

C. AssumeRoleWithWebIdentity

D. GetCallerIdentity

Answer: A

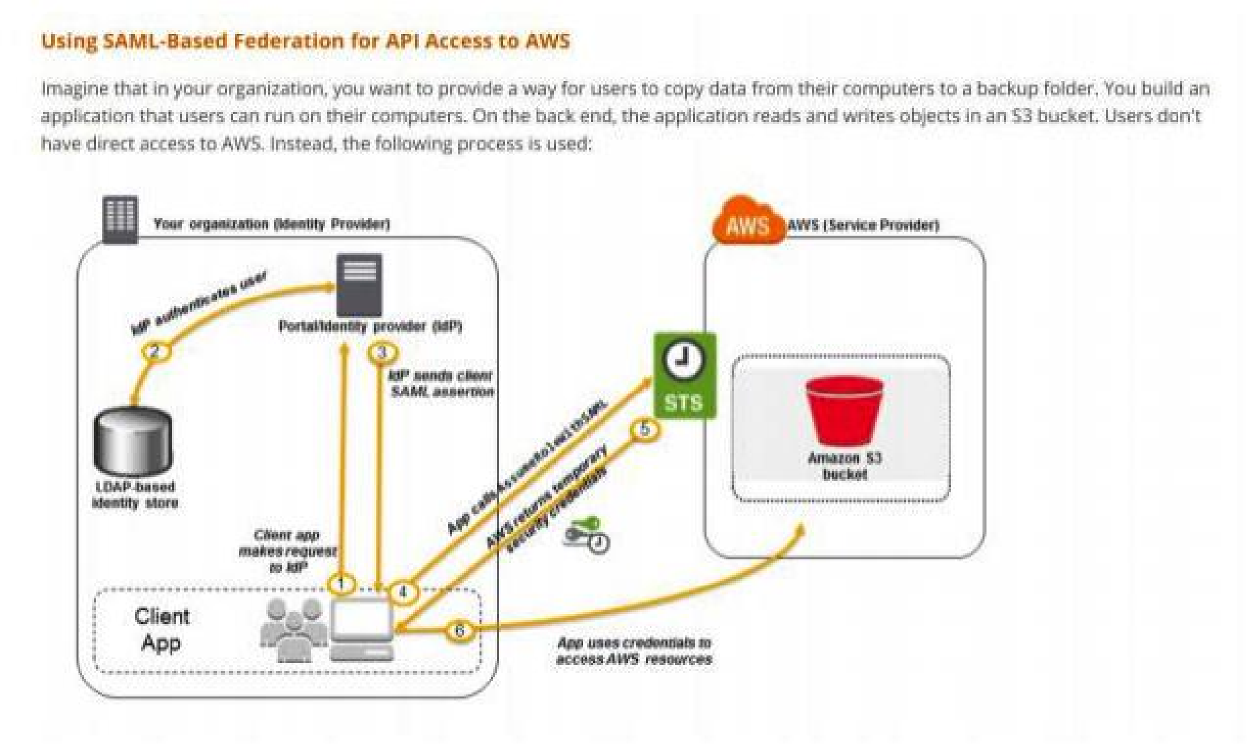


AssumeRoleWithSAML

Returns a set of temporary security credentials for users who have been authenticated via a SAML authentication response. This operation provides a mechanism for tying an enterprise identity store or directory to role-based AWS access without user-specific credentials or configuration. For a comparison of `AssumeRoleWithSAML` with the other API operations that produce temporary credentials, see Requesting Temporary Security Credentials and Comparing the AWS STS API operations in the *IAM User Guide*.

The temporary security credentials returned by this operation consist of an access key ID, a secret access key, and a security token. Applications can use these temporary security credentials to sign calls to AWS services.

https://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRoleWithSAML.html



Using SAML-Based Federation for API Access to AWS

Imagine that in your organization, you want to provide a way for users to copy data from their computers to a backup folder. You build an application that users can run on their computers. On the back end, the application reads and writes objects in an S3 bucket. Users don't have direct access to AWS. Instead, the following process is used:

Your organization (Identity Provider)
AWS
AWS (Service Provider)
IdP authenticates user
2
Portal/Identity provider (IdP)
3
IdP sends client SAML assertion
LDAP-based identity store
STS
5
Amazon S3 bucket
App calls AssumeRoleWithSAML
AWS returns temporary security credentials
Client app makes request to IdP
1
4
Client App
6
App uses credentials to access AWS resources

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

Also Read: Top AWS Solution Architect Interview Questions with Detailed Answers

10. How many VPCs can an Internet Gateway be attached to at any given time?

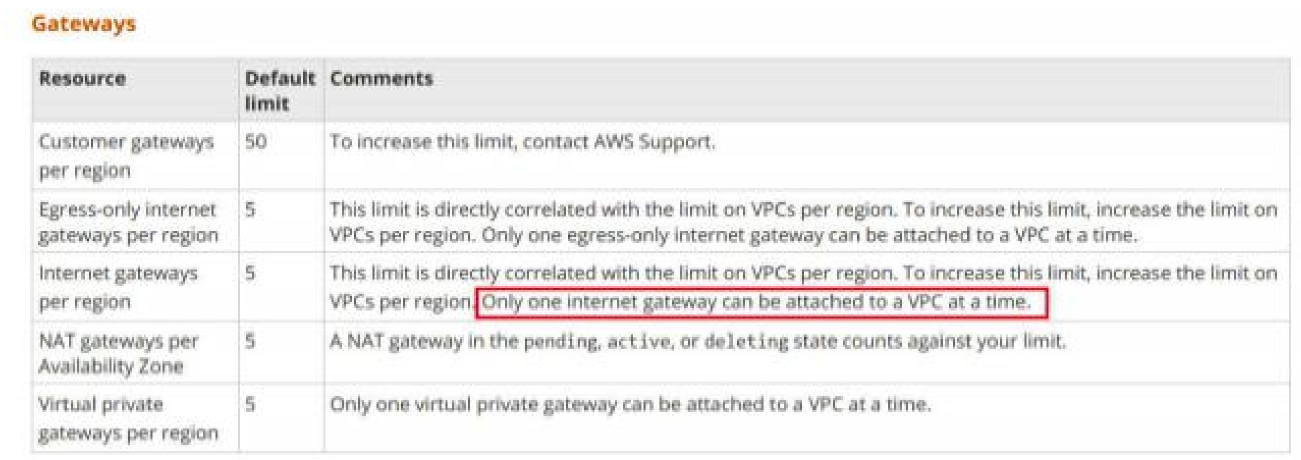
A. 2

B. 5

C. 1

D. By default 1. But it can be attached to any VPC peered with its belonging VPC.

Answer: C

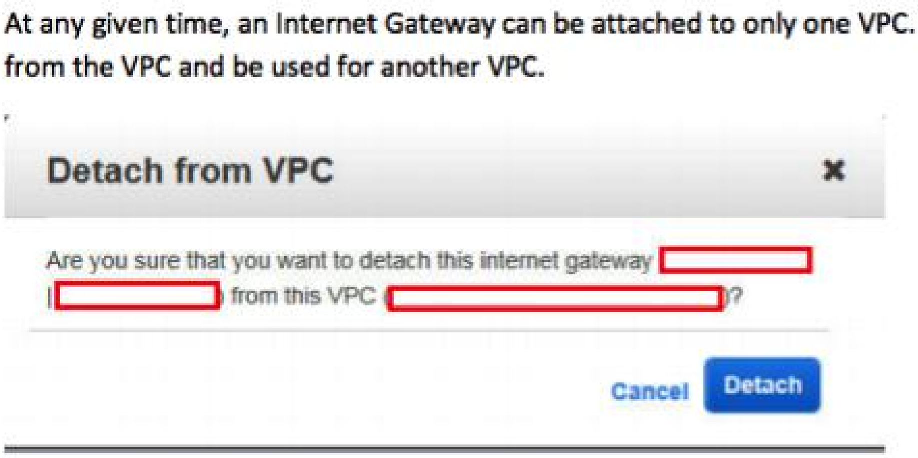


Gateways

Resource	Default limit	Comments
Customer gateways per region	50	To increase this limit, contact AWS Support.
Egress-only internet gateways per region	5	This limit is directly correlated with the limit on VPCs per region. To increase this limit, increase the limit on VPCs per region. Only one egress-only internet gateway can be attached to a VPC at a time.
Internet gateways per region	5	This limit is directly correlated with the limit on VPCs per region. To increase this limit, increase the limit on VPCs per region. Only one internet gateway can be attached to a VPC at a time.
NAT gateways per Availability Zone	5	A NAT gateway in the pending, active, or deleting state counts against your limit.
Virtual private gateways per region	5	Only one virtual private gateway can be attached to a VPC at a time.

https://docs.aws.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html#vpc-limits-gateways

At any given time, an Internet Gateway can be attached to only one VPC. It can be detached from the VPC and be used for another VPC.



At any given time, an Internet Gateway can be attached to only one VPC. It can be detached from the VPC and be used for another VPC.

Are you sure that you want to detach this internet gateway [redacted] ([redacted]) from this VPC ([redacted])?

11. Your organization was planning to develop a web application on AWS EC2. Application admin was tasked to perform AWS setup required to spin EC2 instance inside an existing private VPC. He/she has created a subnet and wants to ensure no other subnets in the VPC can communicate with your subnet except for the specific IP address. So he/she created a new route table and associated with the new subnet. When he/she was trying to delete the route with the target as local, there is no option to delete the route. What could have caused this behavior?

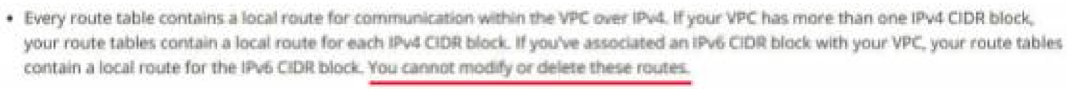
A. Policy attached to IAM user does not have access to remove routes.

B. A route with the target as local cannot be deleted.

C. You cannot add/delete routes when associated with the subnet. Remove associated, add/delete routes and associate again with the subnet.

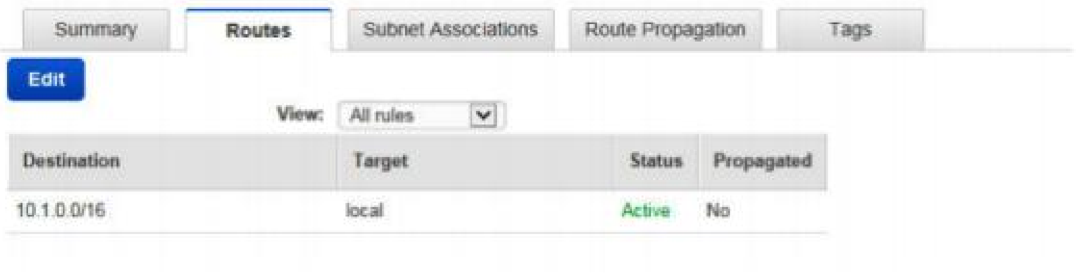
D. There must be at least one route on the route table. Add a new route to enable delete option on existing routes.

Answer: B



- Every route table contains a local route for communication within the VPC over IPv4. If your VPC has more than one IPv4 CIDR block, your route tables contain a local route for each IPv4 CIDR block. If you've associated an IPv6 CIDR block with your VPC, your route tables contain a local route for the IPv6 CIDR block. You cannot modify or delete these routes.

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html#RouteTa



Destination	Target	Status	Propagated
10.1.0.0/16	local	Active	No

12. Which of the following are not backup and restore solutions provided by AWS? (choose multiple)

A. AWS Elastic Block Store

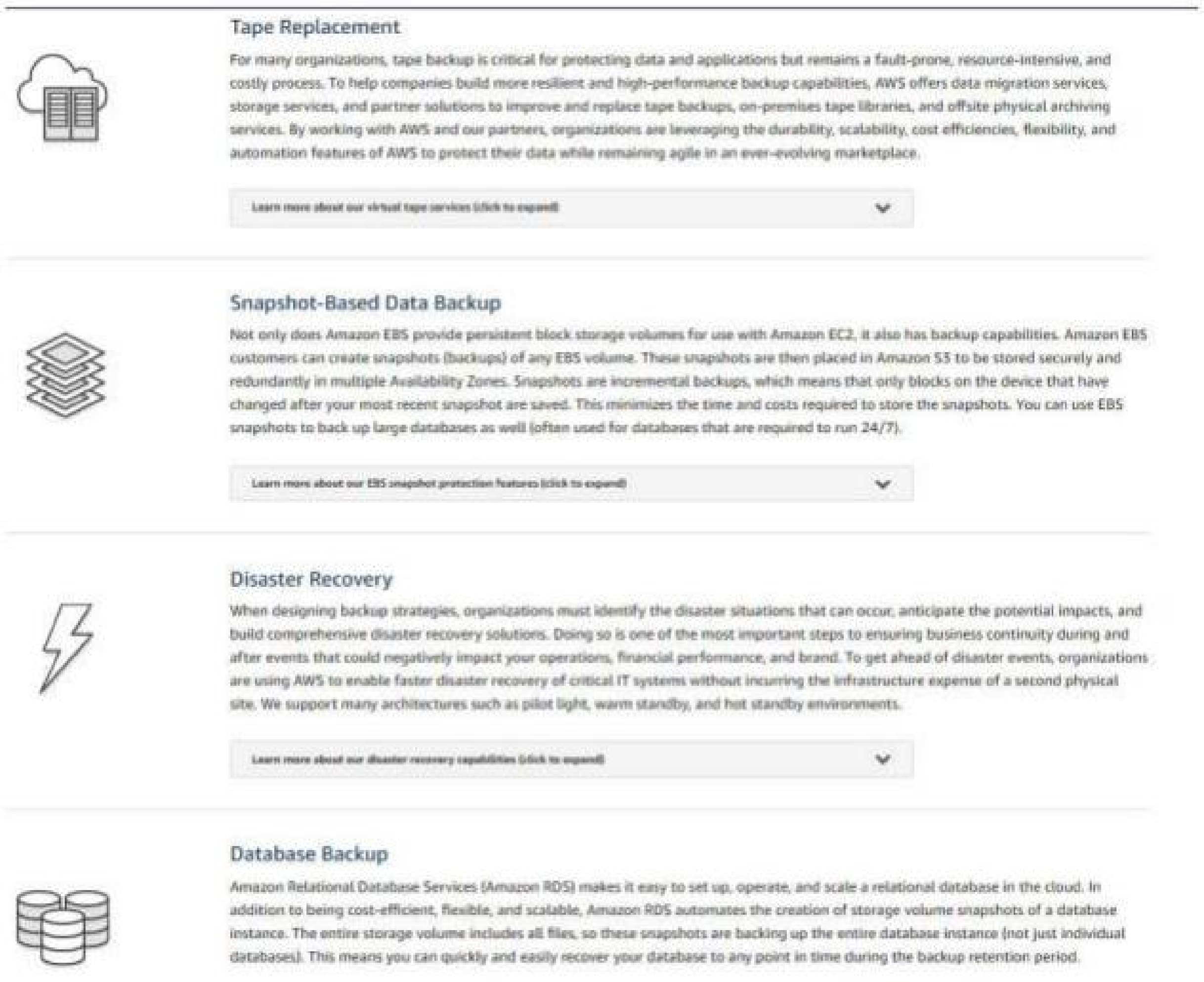
B. AWS Storage Gateway

C. AWS Elastic Beanstalk

D. AWS Database Migration Hub

E. AWS CloudFormation

Answer: C, E



Tape Replacement

For many organizations, tape backup is critical for protecting data and applications but remains a fault-prone, resource-intensive, and costly process. To help companies build more resilient and high-performance backup capabilities, AWS offers data migration services, storage services, and partner solutions to improve and replace tape backups, on-premises tape libraries, and offsite physical archiving services. By working with AWS and our partners, organizations are leveraging the durability, scalability, cost efficiencies, flexibility, and automation features of AWS to protect their data while remaining agile in an ever-evolving marketplace.

Learn more about our virtual tape services (click to expand)

Snapshot-Based Data Backup

Not only does Amazon EBS provide persistent block storage volumes for use with Amazon EC2, it also has backup capabilities. Amazon EBS customers can create snapshots (backups) of any EBS volume. These snapshots are then placed in Amazon S3 to be stored securely and redundantly in multiple Availability Zones. Snapshots are incremental backups, which means that only blocks on the device that have changed after your most recent snapshot are saved. This minimizes the time and costs required to store the snapshots. You can use EBS snapshots to back up large databases as well (often used for databases that are required to run 24/7).

Learn more about our EBS snapshot protection features (click to expand)

Disaster Recovery

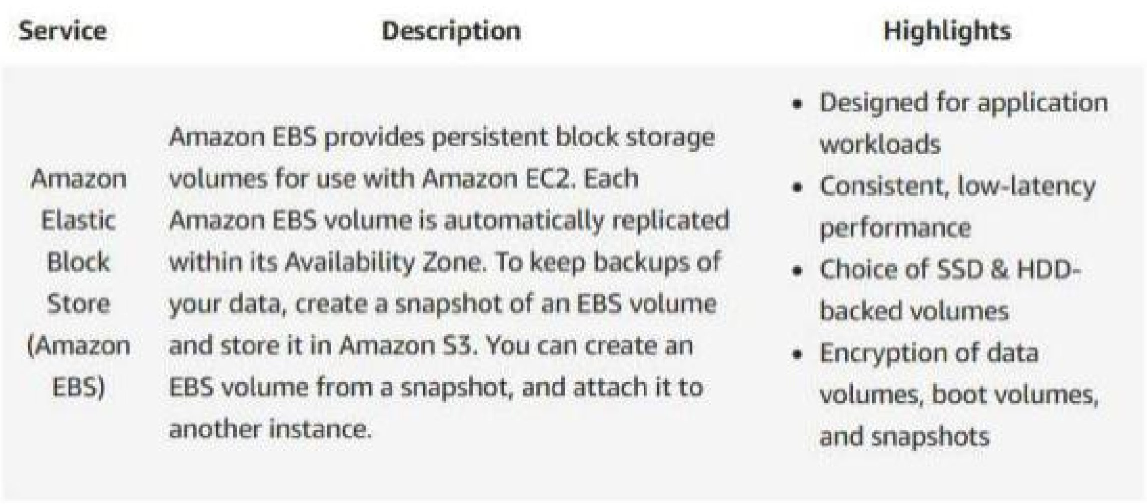
When designing backup strategies, organizations must identify the disaster situations that can occur, anticipate the potential impacts, and build comprehensive disaster recovery solutions. Doing so is one of the most important steps to ensuring business continuity during and after events that could negatively impact your operations, financial performance, and brand. To get ahead of disaster events, organizations are using AWS to enable faster disaster recovery of critical IT systems without incurring the infrastructure expense of a second physical site. We support many architectures such as pilot light, warm standby, and hot standby environments.

Learn more about our disaster recovery capabilities (click to expand)

Database Backup

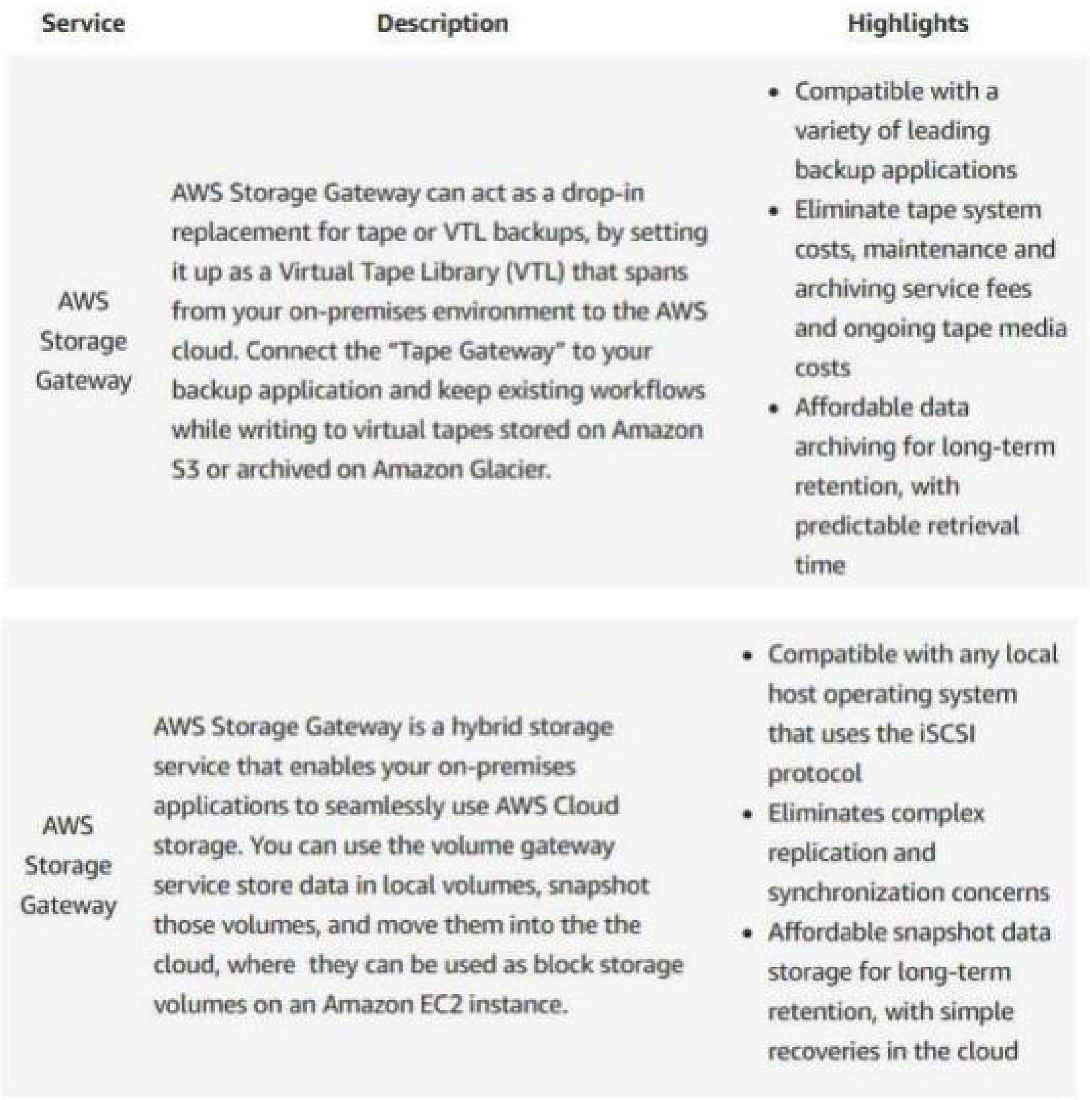
Amazon Relational Database Services (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. In addition to being cost-efficient, flexible, and scalable, Amazon RDS automates the creation of storage volume snapshots of a database instance. The entire storage volume includes all files, so these snapshots are backing up the entire database instance (not just individual databases). This means you can quickly and easily recover your database to any point in time during the backup retention period.

Option A is snapshot based data backup solution.



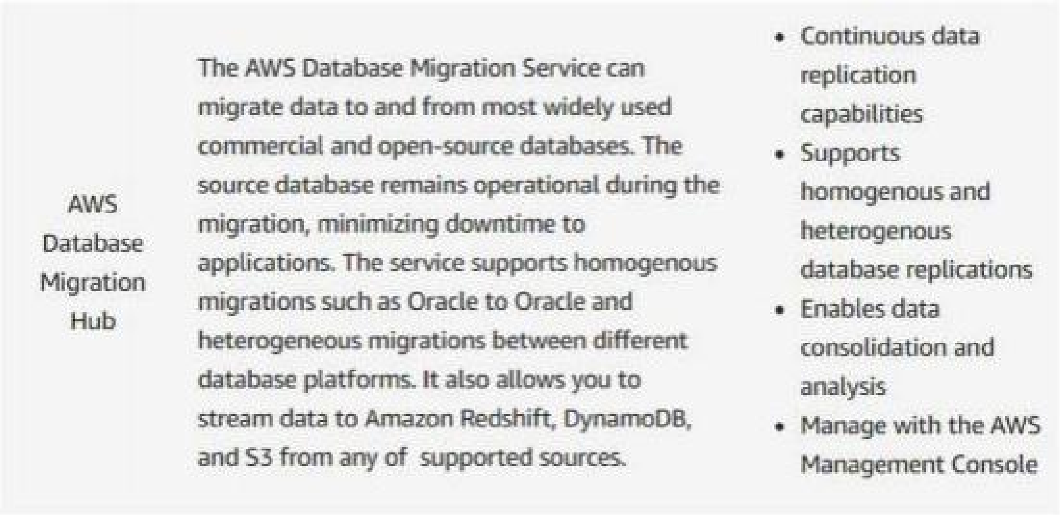
Service	Description	Highlights
Amazon Elastic Block Store (Amazon EBS)	Amazon EBS provides persistent block storage volumes for use with Amazon EC2. Each Amazon EBS volume is automatically replicated within its Availability Zone. To keep backups of your data, create a snapshot of an EBS volume and store it in Amazon S3. You can create an EBS volume from a snapshot, and attach it to another instance.	• Designed for application workloads • Consistent, low-latency performance • Choice of SSD & HDD-backed volumes • Encryption of data volumes, boot volumes, and snapshots

Option B, AWS Storage Gateway provides multiple solutions for backup & recovery.



Service	Description	Highlights
AWS Storage Gateway	AWS Storage Gateway can act as a drop-in replacement for tape or VTL backups, by setting it up as a Virtual Tape Library (VTL) that spans from your on-premises environment to the AWS cloud. Connect the "Tape Gateway" to your backup application and keep existing workflows while writing to virtual tapes stored on Amazon S3 or archived on Amazon Glacier.	• Compatible with a variety of leading backup applications • Eliminate tape system costs, maintenance and archiving service fees and ongoing tape media costs • Affordable data archiving for long-term retention, with predictable retrieval time
AWS Storage Gateway	AWS Storage Gateway is a hybrid storage service that enables your on-premises applications to seamlessly use AWS Cloud storage. You can use the volume gateway service store data in local volumes, snapshot those volumes, and move them into the the cloud, where they can be used as block storage volumes on an Amazon EC2 instance.	• Compatible with any local host operating system that uses the iSCSI protocol • Eliminates complex replication and synchronization concerns • Affordable snapshot data storage for long-term retention, with simple recoveries in the cloud

Option D can be used as a Database backup solution.



AWS Database Migration Hub	The AWS Database Migration Service can migrate data to and from most widely used commercial and open-source databases. The source database remains operational during the migration, minimizing downtime to applications. The service supports homogenous migrations such as Oracle to Oracle and heterogeneous migrations between different database platforms. It also allows you to stream data to Amazon Redshift, DynamoDB, and S3 from any of supported sources.	• Continuous data replication capabilities • Supports homogenous and heterogenous database replications • Enables data consolidation and analysis • Manage with the AWS Management Console

13. Organization ABC has a requirement to send emails to multiple users from their application deployed on EC2 instance in a private VPC. Email receivers will not be IAM users. You have decided to use AWS Simple Email Service and configured from email address. You are using AWS SES API to send emails from your EC2 instance to multiple users. However, email sending getting failed. Which of the following options could be the reason?

A. You have not created VPC endpoint for SES service and configured in the route table.

B. AWS SES is in sandbox mode by default which can send emails only to verified email addresses.

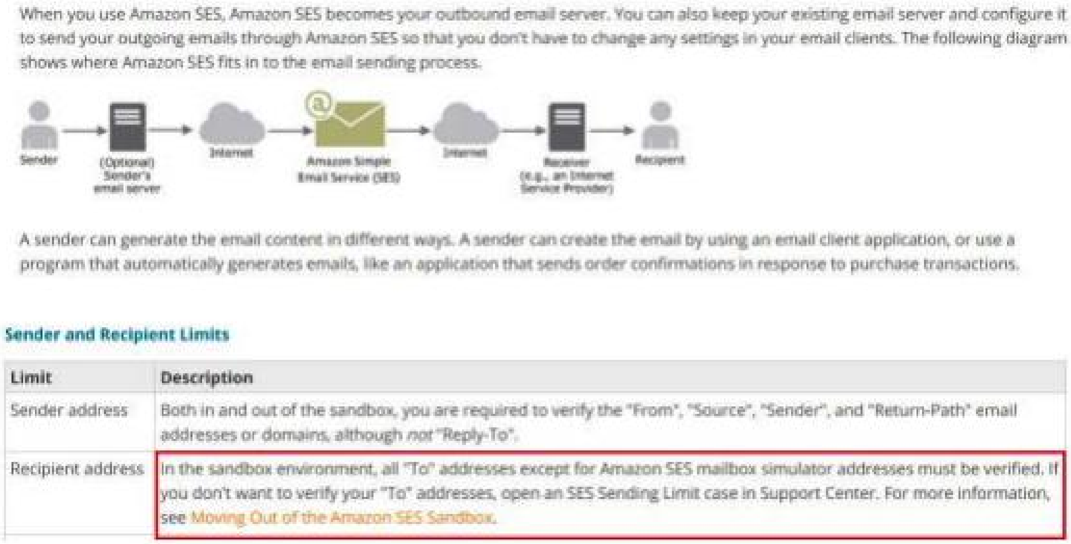
C. IAM user of configured from email address does not have access AWS SES to send emails.

D. AWS SES cannot send emails to addresses which are not configured as IAM users. You have to use the SMTP service provided by AWS.

Answer: B

Amazon SES is an email platform that provides an easy, cost-effective way for you to send and receive email using your own email addresses and domains.

For example, you can send marketing emails such as special offers, transactional emails such as order confirmations, and other types of correspondence such as newsletters. When you use Amazon SES to receive mail, you can develop software solutions such as email autoresponders, email unsubscribe systems and applications that generate customer support tickets from incoming emails.



When you use Amazon SES, Amazon SES becomes your outbound email server. You can also keep your existing email server and configure it to send your outgoing emails through Amazon SES so that you don't have to change any settings in your email clients. The following diagram shows where Amazon SES fits in to the email sending process.

Sender
(Optional) Sender's email server
Internet
Amazon Simple Email Service (SES)
Internet
Receiver (e.g., an Internet Service Provider)
Recipient

A sender can generate the email content in different ways. A sender can create the email by using an email client application, or use a program that automatically generates emails, like an application that sends order confirmations in response to purchase transactions.

Sender and Recipient Limits

Limit	Description
Sender address	Both in and out of the sandbox, you are required to verify the "From", "Source", "Sender", and "Return-Path" email addresses or domains, although *not* "Reply-To".
Recipient address	In the sandbox environment, all "To" addresses except for Amazon SES mailbox simulator addresses must be verified. If you don't want to verify your "To" addresses, open an SES Sending Limit case in Support Center. For more information, see Moving Out of the Amazon SES Sandbox.

https://docs.aws.amazon.com/ses/latest/DeveloperGuide/limits.html

https://docs.aws.amazon.com/ses/latest/DeveloperGuide/request-production-access.html

14. You have configured AWS S3 event notification to send a message to AWS Simple Queue Service whenever an object is deleted. You are performing ReceiveMessage API operation on the AWS SQS queue to receive the S3 delete object message onto AWS EC2 instance. For any successful message operations, you are deleting them from the queue. For failed operations, you are not deleting the messages. You have developed a retry mechanism which reruns the application every 5 minutes for failed RecieveMessage operations. However, you are not receiving the messages again during the rerun. What could have caused this?

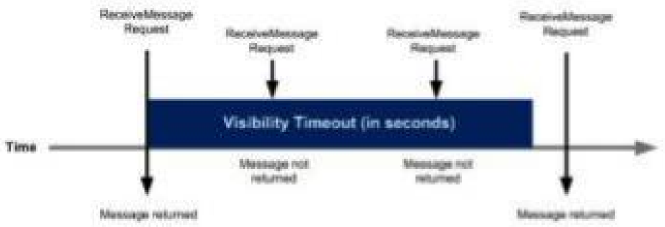
A. AWS SQS deletes the message after it has been read through ReceiveMessage API

B. You are using Long Polling which does not guarantee message delivery.

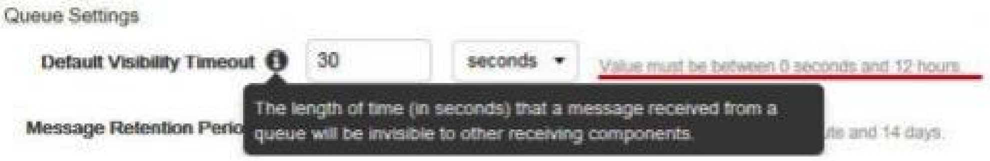
C. Failed RecieveMessage queue messages are automatically sent to Dead Letter Queues. You need to RecieveMessage from Dead Letter Queue for failed retries.

D. Visibility Timeout on the SQS queue is set to 10 minutes.

Answer: D When a consumer receives and processes a message from a queue, the message remains in the queue. Amazon SQS doesn't automatically delete the message. Because Amazon SQS is a distributed system, there's no guarantee that the consumer actually receives the message (for example, due to a connectivity issue, or due to an issue in the consumer application). Thus, the consumer must delete the message from the queue after receiving and processing it.



Immediately after a message is received, it remains in the queue. To prevent other consumers from processing the message again, Amazon SQS sets a *visibility timeout*, a period of time during which Amazon SQS prevents other consumers from receiving and processing the message. The default (minimum) visibility timeout for a message is 30 seconds. The maximum is 12 hours. For information about configuring visibility timeout for a queue using the AWS Management Console and for single or multiple messages using the AWS SDK for Java (and the `SetQueueAttributes`, `GetQueueAttributes`, `ReceiveMessage`, `ChangeMessageVisibility`, and `ChangeMessageVisibilityBatch` actions), see Configuring Visibility Timeout for an Amazon SQS Queue.



Queue Settings

Default Visibility Timeout: 30 seconds — Value must be between 0 seconds and 12 hours

The length of time (in seconds) that a message received from a queue will be invisible to other receiving components.

Message Retention Perio… …te and 14 days.

https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html

15. You had set up an internal HTTP(S) Elastic Load Balancer to route requests to two EC2 instances inside a private VPC. However, one of the target EC2 instance is showing Unhealthy status. Which of the following options could not be a reason for this?

A. Port 80/443 is not allowed on EC2 instance’s Security Group from the load balancer.

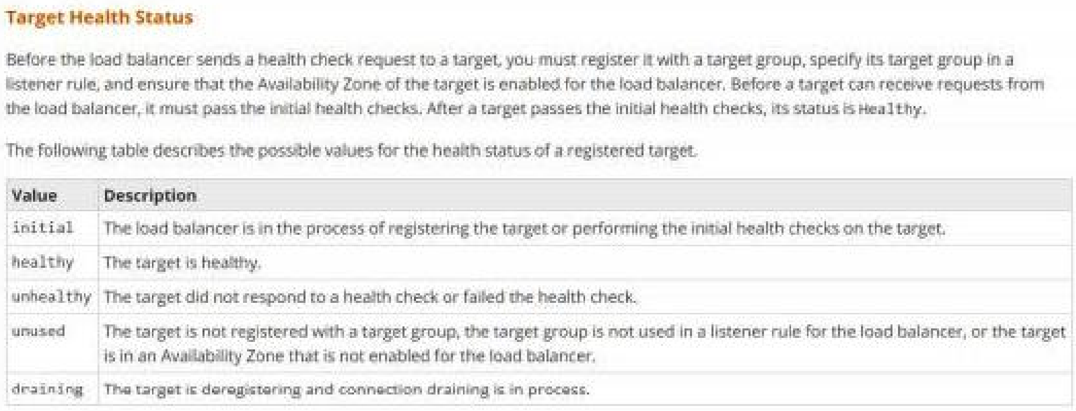
B. An EC2 instance is in different availability zones than load balancer.

C. The ping path does not exist on the EC2 instance.

D. The target did not return a successful response code

Answer: B

If a target is taking longer than expected to enter the InService state, it might be failing health checks. Your target is not in service until it passes one health check.

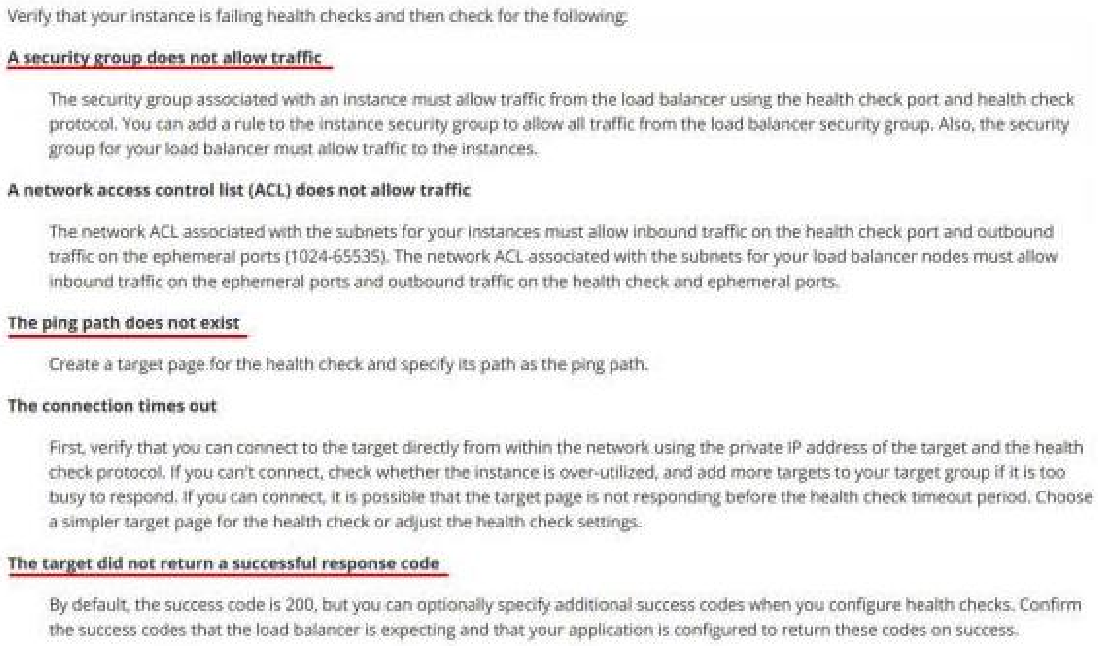


Target Health Status

Before the load balancer sends a health check request to a target, you must register it with a target group, specify its target group in a listener rule, and ensure that the Availability Zone of the target is enabled for the load balancer. Before a target can receive requests from the load balancer, it must pass the initial health checks. After a target passes the initial health checks, its status is `Healthy`.

The following table describes the possible values for the health status of a registered target.

Value	Description
`initial`	The load balancer is in the process of registering the target or performing the initial health checks on the target.
`healthy`	The target is healthy.
`unhealthy`	The target did not respond to a health check or failed the health check.
`unused`	The target is not registered with a target group, the target group is not used in a listener rule for the load balancer, or the target is in an Availability Zone that is not enabled for the load balancer.
`draining`	The target is deregistering and connection draining is in process.



Verify that your instance is failing health checks and then check for the following:

A security group does not allow traffic

The security group associated with an instance must allow traffic from the load balancer using the health check port and health check protocol. You can add a rule to the instance security group to allow all traffic from the load balancer security group. Also, the security group for your load balancer must allow traffic to the instances.

A network access control list (ACL) does not allow traffic

The network ACL associated with the subnets for your instances must allow inbound traffic on the health check port and outbound traffic on the ephemeral ports (1024-65535). The network ACL associated with the subnets for your load balancer nodes must allow inbound traffic on the ephemeral ports and outbound traffic on the health check and ephemeral ports.

The ping path does not exist

Create a target page for the health check and specify its path as the ping path.

The connection times out

First, verify that you can connect to the target directly from within the network using the private IP address of the target and the health check protocol. If you can't connect, check whether the instance is over-utilized, and add more targets to your target group if it is too busy to respond. If you can connect, it is possible that the target page is not responding before the health check timeout period. Choose a simpler target page for the health check or adjust the health check settings.

The target did not return a successful response code

By default, the success code is 200, but you can optionally specify additional success codes when you configure health checks. Confirm the success codes that the load balancer is expecting and that your application is configured to return these codes on success.

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-troubleshooting.html#target-not-inservice

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/target-group-health-checks.html

16. Your organization has an existing VPC setup and has a requirement to route any traffic going from VPC to AWS S3 bucket through AWS internal network. So they have created VPC end point for S3 and configured to allow traffic for S3 buckets. The application you are developing involves sending traffic to AWS S3 bucket from VPC for which you planned to use a similar approach. You have created a new route table, added route to VPC endpoint and associated route table with your new subnet. However, when you are trying to send a request from EC2 to S3 bucket using AWS CLI, the request is getting failed with 403 access denied errors. What could be causing the failure?

A. AWS S3 bucket is in the different region than your VPC.

B. EC2 security group outbound rules not allowing traffic to S3 prefix list.

C. VPC endpoint might have a restrictive policy and does not contain the new S3 bucket.

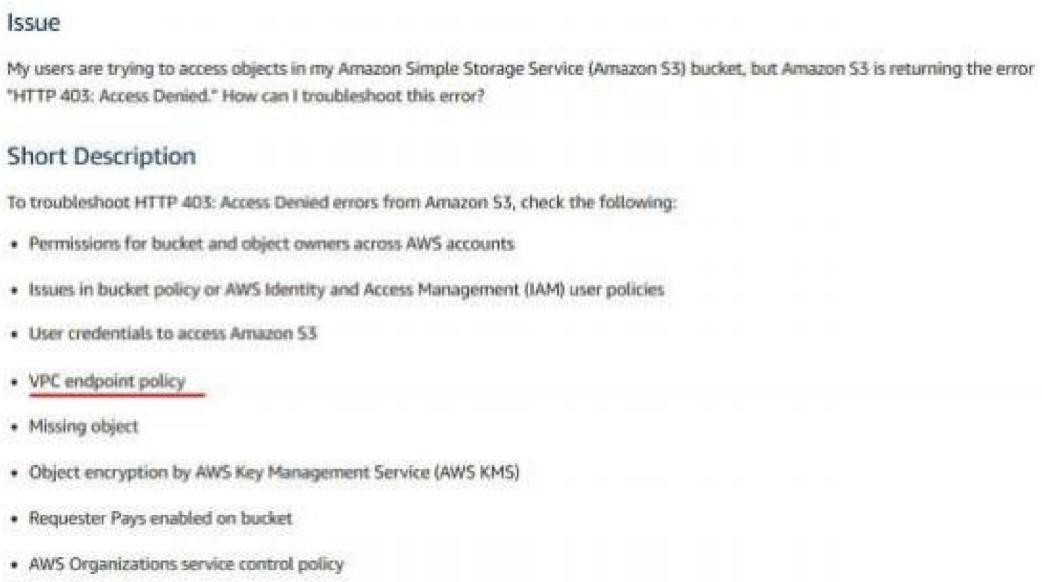
D. S3 bucket CORS configuration does not have EC2 instance as the origin.

Answer: C

Option A is not correct. The question states “403 access denied”. If the S3 bucket is in a different region than VPC, the request looks for a route with NAT Gateway or Internet Gateway. If exists, the request goes through the internet to S3. If does not exist, the request gets failed with connection refused or connection timed out. Not with an error “403 access denied”.

Option B is not correct. Same as above, when the security group does not allow traffic, the failure cause will be 403 access denied.

Option C is correct.



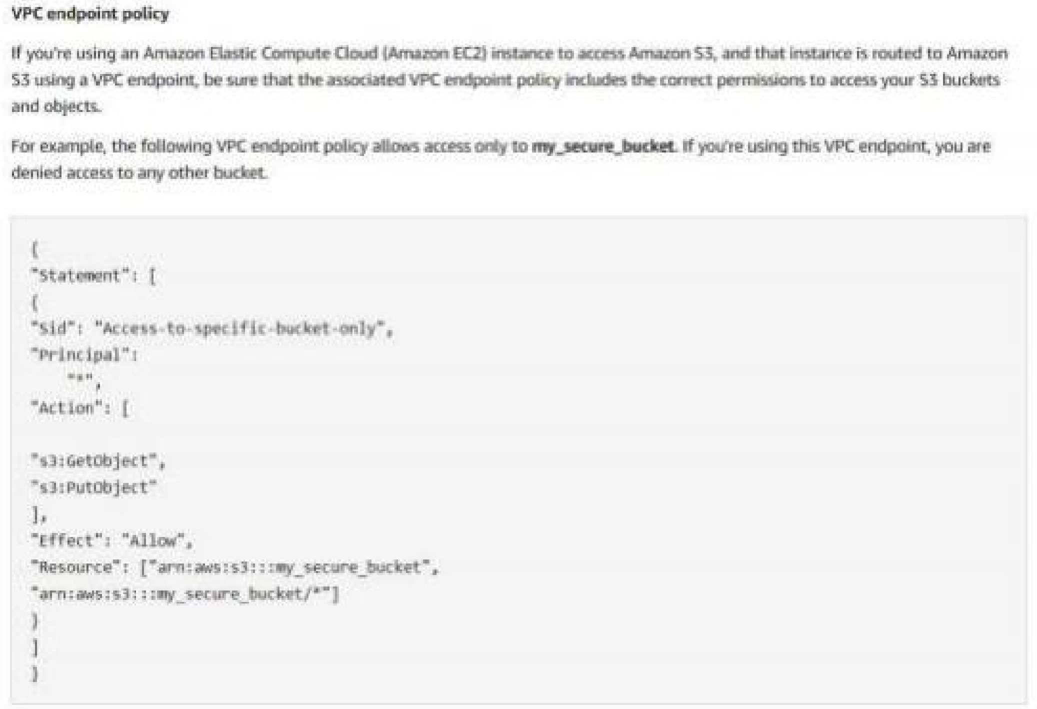
Issue

My users are trying to access objects in my Amazon Simple Storage Service (Amazon S3) bucket, but Amazon S3 is returning the error "HTTP 403: Access Denied." How can I troubleshoot this error?

Short Description

To troubleshoot HTTP 403: Access Denied errors from Amazon S3, check the following:

- Permissions for bucket and object owners across AWS accounts
- Issues in bucket policy or AWS Identity and Access Management (IAM) user policies
- User credentials to access Amazon S3
- VPC endpoint policy
- Missing object
- Object encryption by AWS Key Management Service (AWS KMS)
- Requester Pays enabled on bucket
- AWS Organizations service control policy



VPC endpoint policy

If you're using an Amazon Elastic Compute Cloud (Amazon EC2) instance to access Amazon S3, and that instance is routed to Amazon S3 using a VPC endpoint, be sure that the associated VPC endpoint policy includes the correct permissions to access your S3 buckets and objects.

For example, the following VPC endpoint policy allows access only to **my_secure_bucket**. If you're using this VPC endpoint, you are denied access to any other bucket.

```
{
"Statement": [
{
"Sid": "Access-to-specific-bucket-only",
"Principal":
    "*",
"Action": [

"s3:GetObject",
"s3:PutObject"
],
"Effect": "Allow",
"Resource": ["arn:aws:s3:::my_secure_bucket",
"arn:aws:s3:::my_secure_bucket/*"]
}
]
}
```

Option D is not correct.

Cross-origin resource sharing (CORS) defines a way for client web applications that are loaded in one domain to interact with resources in a different domain. With CORS support, you can build rich client-side web applications with Amazon S3 and selectively allow cross-origin access to your Amazon S3 resources.

In this case, the request is not coming from a web client.

17. You have launched an RDS instance with MySQL database with default configuration for your file sharing application to store all the transactional information. Due to security compliance, your organization wants to encrypt all the databases and storage on the cloud. They approached you to perform this activity on your MySQL RDS database. How can you achieve this?

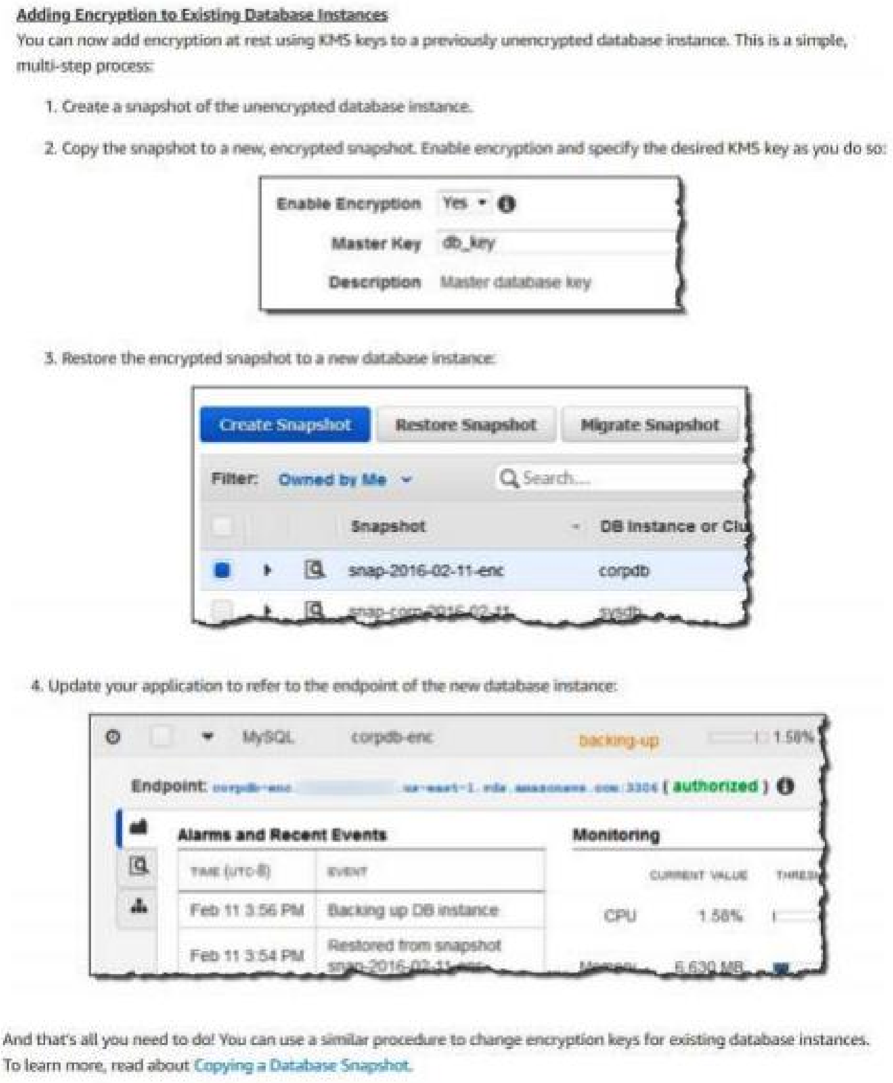
A. Copy snapshot from latest snapshot of your RDS instance, select encryption during copy and restore a new DB instance from the newly encrypted snapshot.

B. Stop the RDS instance, modify and select encryption option. Start the RDS instance, it may take a while to start RDS instance as existing data is getting encrypted.

C. Create a case with AWS support to enable encryption for your RDS instance.

D. AWS RDS is a managed service and the data at rest in all RDS instances are encrypted by default.

Answer: A



Adding Encryption to Existing Database Instances

You can now add encryption at rest using KMS keys to a previously unencrypted database instance. This is a simple, multi-step process:

1. Create a snapshot of the unencrypted database instance.
2. Copy the snapshot to a new, encrypted snapshot. Enable encryption and specify the desired KMS key as you do so:

Enable Encryption: Yes
Master Key: db_key
Description: Master database key

3. Restore the encrypted snapshot to a new database instance:

Snapshot	DB Instance or Clu
snap-2016-02-11-enc	corpdb
snap-corp-2016-02-11	sysdb

4. Update your application to refer to the endpoint of the new database instance:

MySQL corpdb-enc backing-up 1.58%

Endpoint: corpdb-enc [redacted] us-east-1.rds.amazonaws.com:3306 (authorized)

Alarms and Recent Events

TIME (UTC-8)	EVENT
Feb 11 3:56 PM	Backing up DB instance
Feb 11 3:54 PM	Restored from snapshot snap-2016-02-11-enc

Monitoring

	CURRENT VALUE	THRESH
CPU	1.58%	
Memory	6,630 MB	

And that's all you need to do! You can use a similar procedure to change encryption keys for existing database instances. To learn more, read about Copying a Database Snapshot.

https://aws.amazon.com/blogs/aws/amazon-rds-update-share-encrypted-snapshots-encrypt-existing-instances/

18. Which of the following is an AWS component which consumes resources from your VPC?

A. Internet Gateway

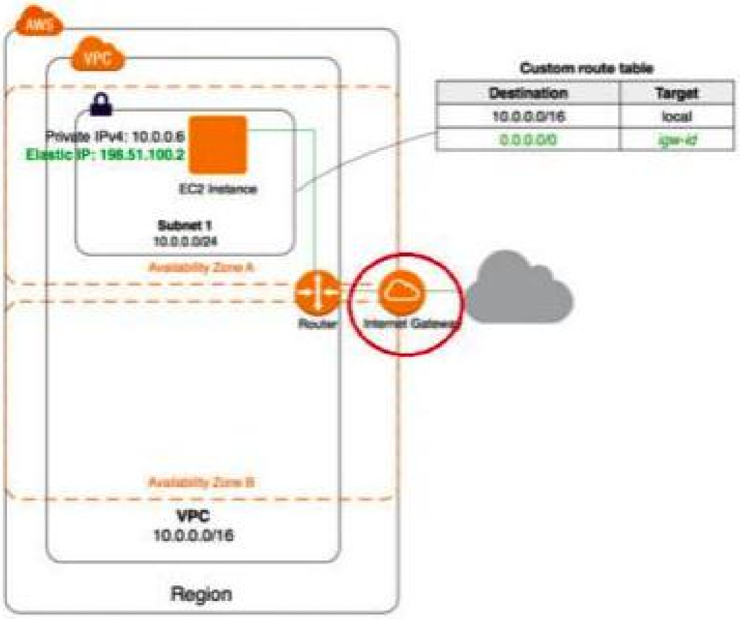
B. Gateway VPC Endpoints

C. Elastic IP Addresses

D. NAT Gateway

Answer: D

Option A is not correct.



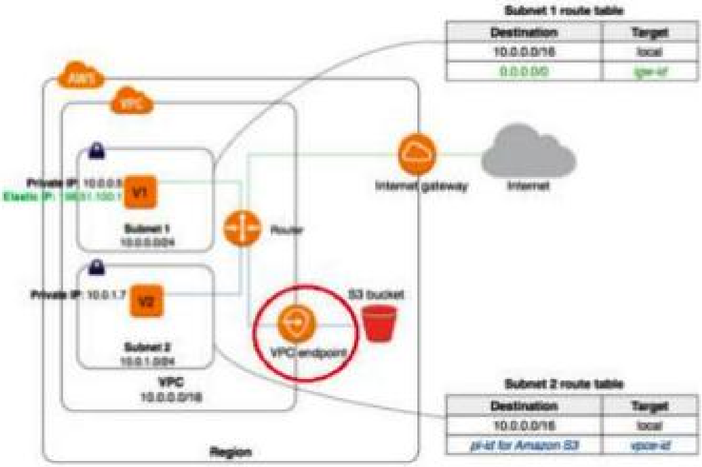
Custom route table

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

An internet gateway is an AWS component which sits outside of your VPC does not consume any resources from your VPC.

Option B is not correct.

Endpoints are virtual devices. They are horizontally scaled, redundant, and highly available VPC components that allow communication between instances in your VPC and services without imposing availability risks or bandwidth constraints on your network traffic.



Subnet 1 route table

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

Subnet 2 route table

Destination	Target
10.0.0.0/16	local
pl-id for Amazon S3	vpce-id

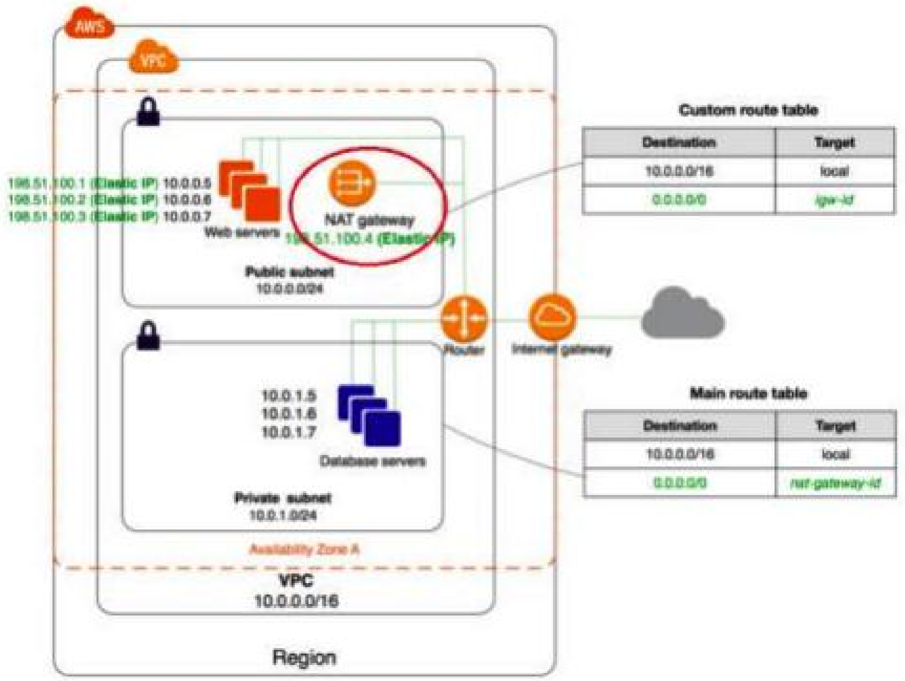
Option C is not correct.

An Elastic IP address is a static, public IPv4 address designed for dynamic cloud computing. You can associate an Elastic IP address with any instance or network interface for any VPC in your account. With an Elastic IP address, you can mask the failure of an instance by rapidly remapping the address to another instance in your VPC.

They do not belong to a single VPC.

Option D is correct.

To create a NAT gateway, you must specify the public subnet in which the NAT gateway should reside. For more information about public and private subnets, see Subnet Routing. You must also specify an Elastic IP address to associate with the NAT gateway when you create it. After you've created a NAT gateway, you must update the route table associated with one or more of your private subnets to point Internet-bound traffic to the NAT gateway. This enables instances in your private subnets to communicate with the internet.



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

19. You have successfully set up a VPC peering connection in your account between two VPCs – VPC A and VPC B, each in a different region. When you are trying to make a request from VPC A to VPC B, request getting failed. Which of the following could be a reason?

A. Cross region peering is not supported in AWS.

B. CIDR blocks of both VPCs might be overlapping.

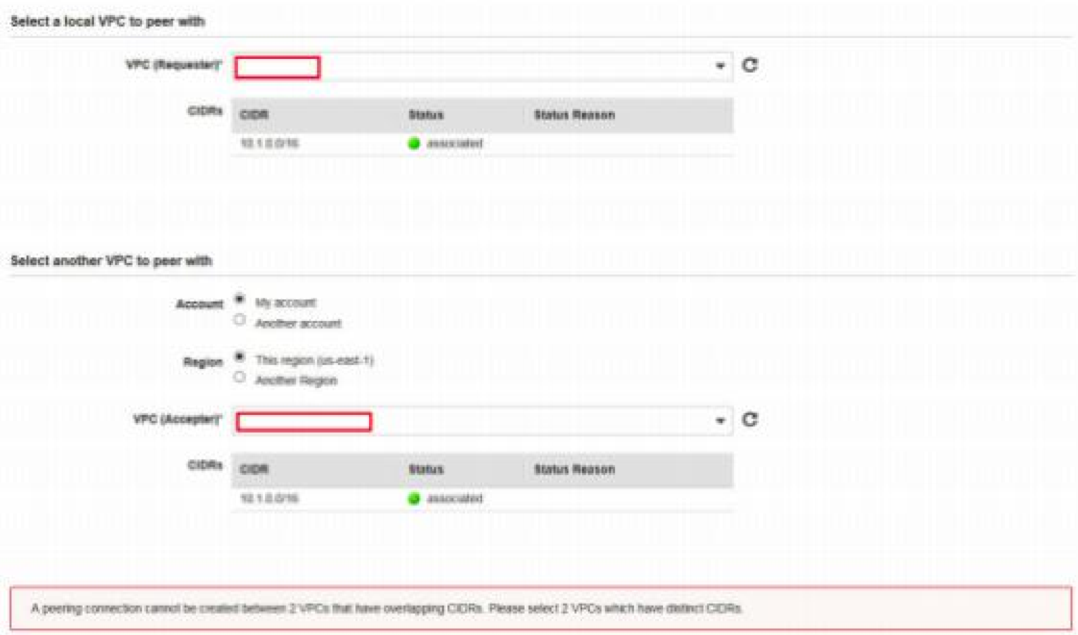
C. Routes not configured in route tables for peering connections.

D. VPC A security group default outbound rules not allowing traffic to VPC B IP range.

Answer: C

Option A is not correct. Cross region VPC peering is supported in AWS.

Option B is not correct.



Select a local VPC to peer with

VPC (Requester)*

CIDRs

CIDR	Status	Status Reason
10.1.0.0/16	● associated	

Select another VPC to peer with

Account ● My account
○ Another account

Region ● This region (us-east-1)
○ Another Region

VPC (Accepter)*

CIDRs

CIDR	Status	Status Reason
10.1.0.0/16	● associated	

A peering connection cannot be created between 2 VPCs that have overlapping CIDRs. Please select 2 VPCs which have distinct CIDRs.

When the VPC IP CIDR blocks are overlapping, you cannot create a peering connection. Question states the peering connection was successful.

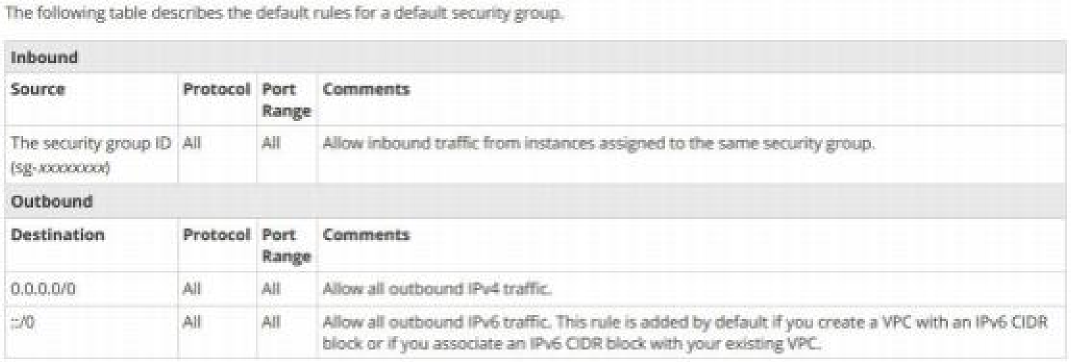
Option C is correct.

To send private IPv4 traffic from your instance to an instance in a peer VPC, you must add a route to the route table that's associated with your subnet in which your instance resides. The route points to the CIDR block (or portion of the CIDR block) of the peer VPC in the VPC peering connection.

https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-routing.html

Option D is not correct.

A security group's default outbound rule allows all traffic going out from the resources attached to the security group.



The following table describes the default rules for a default security group.

Inbound			
Source	**Protocol**	**Port Range**	**Comments**
The security group ID (sg-*xxxxxxxx*)	All	All	Allow inbound traffic from instances assigned to the same security group.
Outbound			
Destination	**Protocol**	**Port Range**	**Comments**
0.0.0.0/0	All	All	Allow all outbound IPv4 traffic.
::/0	All	All	Allow all outbound IPv6 traffic. This rule is added by default if you create a VPC with an IPv6 CIDR block or if you associate an IPv6 CIDR block with your existing VPC.

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

20. Which of the following statements are true in terms of allowing/denying traffic from/to VPC assuming the default rules are not in effect? (choose multiple)

A. In a Network ACL, for a successful HTTPS connection, add an inbound rule with HTTPS type, IP range in source and ALLOW traffic.

B. In a Network ACL, for a successful HTTPS connection, you must add an inbound rule and outbound rule with HTTPS type, IP range in source and destination respectively and ALLOW traffic.

C. In a Security Group, for a successful HTTPS connection, add an inbound rule with HTTPS type and IP range in the source.

D. In a Security Group, for a successful HTTPS connection, you must add an inbound rule and outbound rule with HTTPS type, IP range in source and destination respectively.

Answer: B, C

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; responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa).

Option A is not correct. NACL must have an outbound rule defined for a successful connection due to its stateless nature.

Option B is correct.

Option C is correct.

Configuring an inbound rule in security group is enough for a successful connection due to is stateful nature.

Option D is not correct.

Configuring an outbound rule for incoming connection is not required in security groups.

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

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

21. Which of the following approaches provides the lowest cost for Amazon elastic block store snapshots while giving you the ability to fully restore data?

A. Maintain two snapshots: the original snapshot and the latest incremental snapshot.

B. Maintain a volume snapshot; subsequent snapshots will overwrite one another.

C. Maintain a single snapshot; the latest snapshot is both incremental and complete.

D. Maintain the most current snapshot; archive the original and increment to Amazon Glacier.

Answer: A

After writing data to an EBS volume, you can periodically create a snapshot of the volume to use as a baseline for new volumes or for data backup. If you make periodic snapshots of a volume, the snapshots are incremental which means only the blocks on the device that have changed after your last snapshot are saved in the new snapshot. Even though snapshots are saved incrementally, the snapshot deletion process is designed such that you need to retain only the most recent snapshot in order to restore the volume.