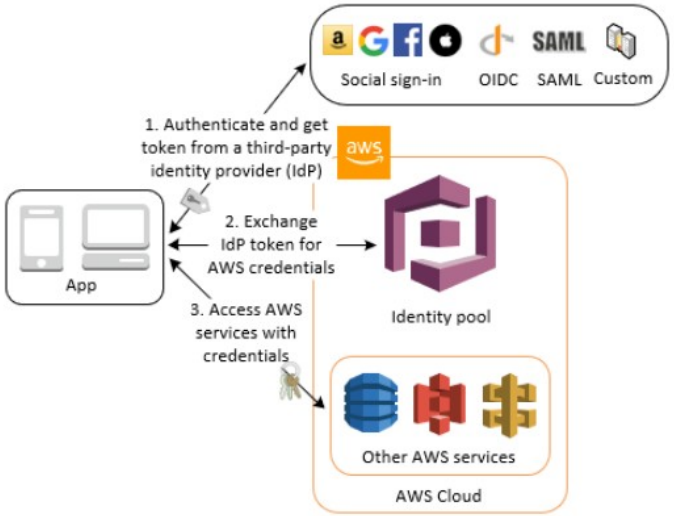
CSAA Practice Test-4

Authenticate with a third party and access AWS services with an identity pool

You can enable your users access to AWS services through an identity pool. An identity pool requires an IdP token from a user that's authenticated by a third-party identity provider (or nothing if it's an anonymous guest). In exchange, the identity pool grants temporary AWS credentials that you can use to access other AWS services. For more information, see **Getting started with Amazon Cognito identity pools (federated identities)**.



https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-scenarios.html
https://docs.aws.amazon.com/cognito/latest/developerguide/identity-pools.html#enable-or-disable-unauthenticated-identities

Q-1

OAuth 2.0 vs OpenID Connect vs SAML

Remember that it isn't a question of which structure an organization should use, but rather of when each one should be deployed. A strong identity solution will use these three structures to achieve different ends, depending on the kind of operations an enterprise needs to protect. Their use cases are as follows:

OAuth 2.0: If you've ever signed up to a new application and agreed to let it automatically source new contacts via Facebook or your phone contacts, then you've likely used OAuth 2.0. This standard provides secure delegated access. That means an application can take actions or access resources from a server on behalf of the user, without them having to share their credentials. It does this by allowing the **identity provider (IdP)** to issue tokens to third-party applications with the user's approval.

OpenID Connect: If you've used your Google to sign in to applications like YouTube, or Facebook to log into an online shopping cart, then you're familiar with this authentication option. OpenID Connect is an open standard that organizations use to authenticate users. IdPs use this so that users can sign in to the IdP, and then access other websites and apps without having to log in or share their sign-in information.

SAML: You've more likely experienced SAML authentication in action in the work environment. For example, it enables you to log into your corporate intranet or IdP and then access numerous additional services, such as Salesforce, Box, or Workday, without having to re-enter your credentials. SAML is an XML-based standard for exchanging authentication and authorization data between IdPs and service providers to verify the user's identity and permissions, then grant or deny their access to services.

Enterprises rely on web frameworks and protocols like OAuth 2.0, OpenID, and SAML to bring structure and security to federated identity. Knowing when to use each is a key step towards protecting your organization's data from the ground up.

https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pools-oidc-idp.html

Q-2

CloudFront compliance best practices

This section provides best practices and recommendations for compliance when you use Amazon CloudFront to serve your content.

If you run PCI-compliant or HIPAA-compliant workloads that are based on the **AWS shared responsibility model**, we recommend that you log your CloudFront usage data for the last 365 days for future auditing purposes. To log usage data, you can do the following:

- Enable CloudFront access logs. For more information, see **Configuring and using standard logs (access logs)**.
- Capture requests that are sent to the CloudFront API. For more information, see **Using AWS CloudTrail to capture requests sent to the CloudFront API**.

In addition, see the following for details about how CloudFront is compliant with the PCI DSS and SOC standards.

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

Q-3

	Interface Endpoint	Gateway Endpoint
What	Elastic Network Interface with a Private IP	A gateway that is a target for a specific route
How	Uses DNS entries to redirect traffic	Uses prefix lists in the route table to redirect traffic
Which services	API Gateway, CloudFormation, CloudWatch etc.	Amazon S3, DynamoDB
Security	Security Groups	VPC Endpoint Policies

Q-4

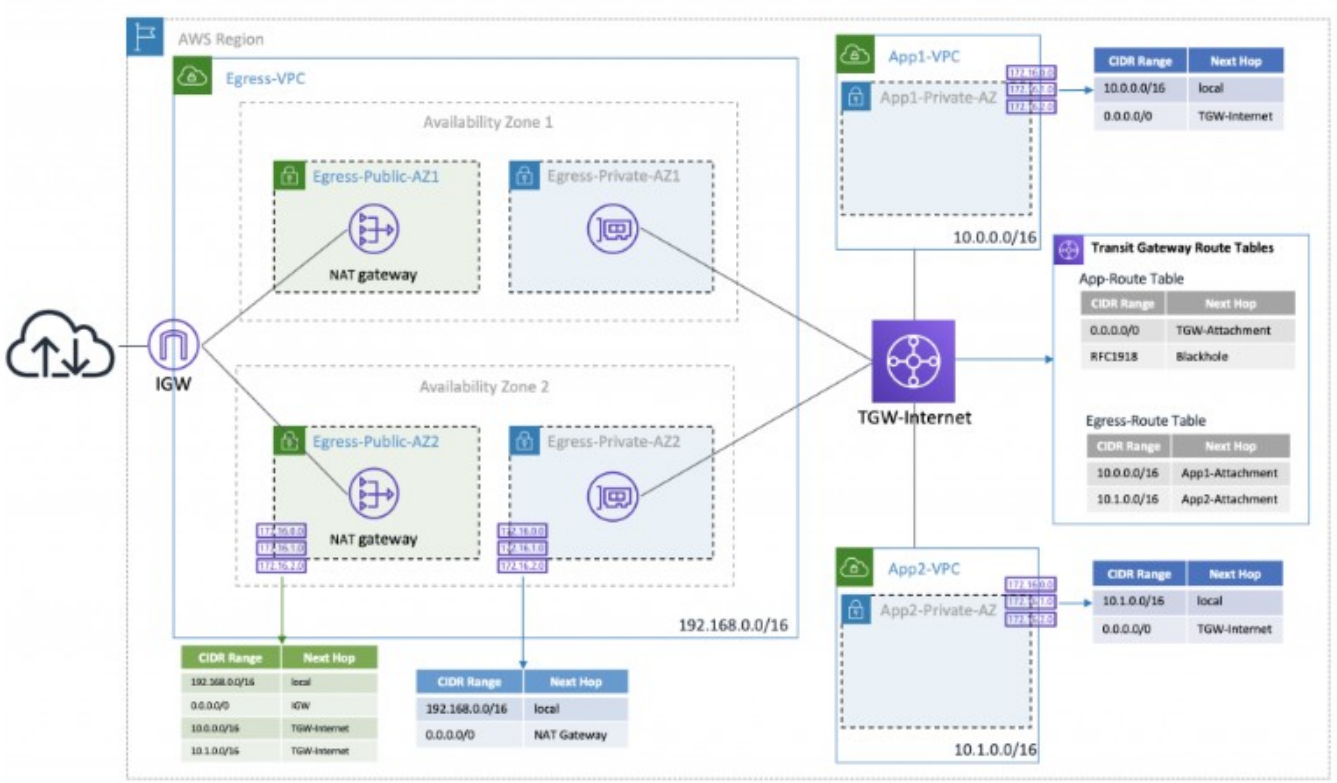
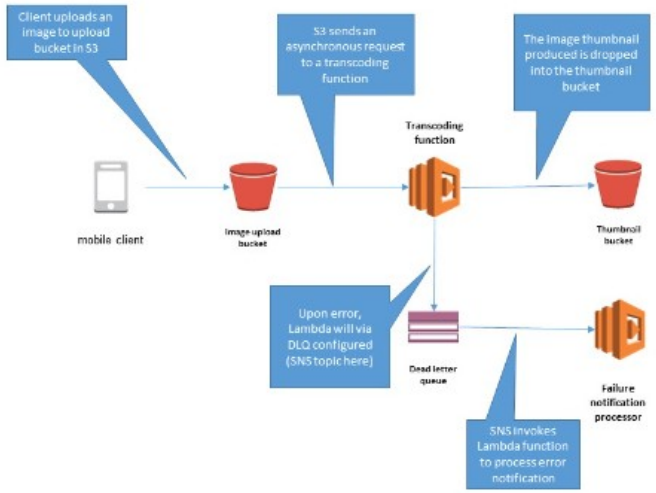


Figure 1: Architecture diagram showing AWS Transit Gateway to centralize outbound internet traffic from multiple VPCs

https://aws.amazon.com/blogs/networking-and-content-delivery/creating-a-single-internet-exit-point-from-multiple-vpcs-using-aws-transit-gateway/

Q-5

Take the typical beginner use case for learning about serverless applications on AWS: creating thumbnails from images dropped onto an S3 bucket. The transcoding Lambda function can be configured to send any transcoding failures to an SNS topic, which triggers a Lambda function for further investigation.



Now, you can set up a dead letter queue for an existing Lambda function and test out the feature.

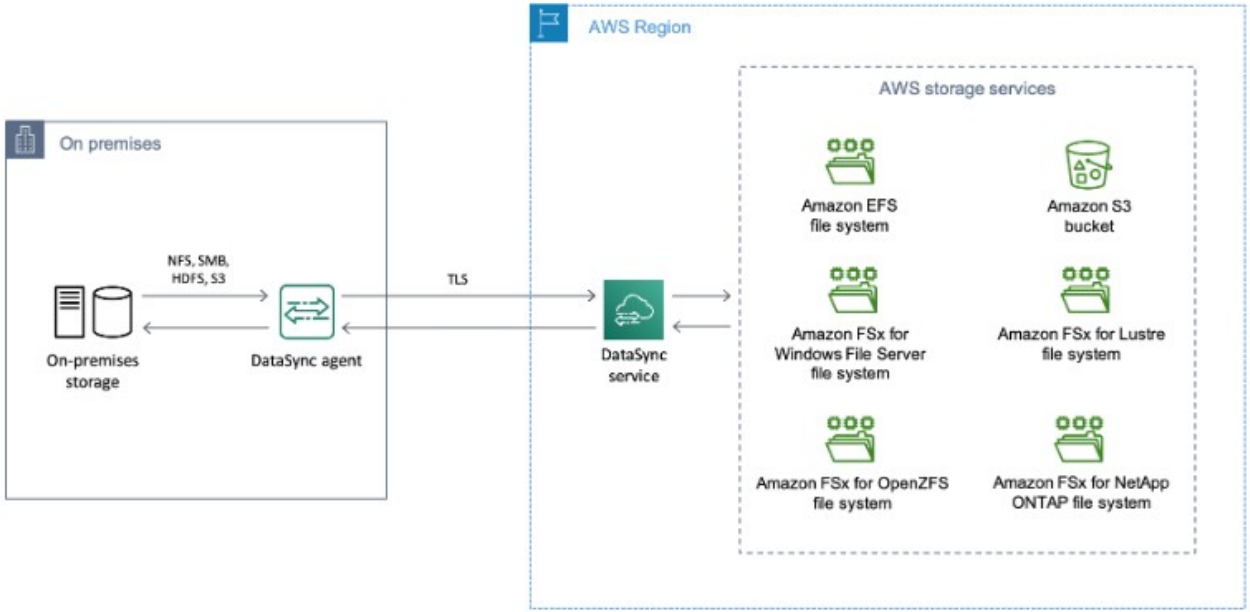
https://docs.aws.amazon.com/lambda/latest/dg/invocation-async.html?icmpid=docs_lambda_help#invocation-async-destinations

https://aws.amazon.com/blogs/compute/robust-serverless-application-design-with-aws-lambda-dlq/

Q-6

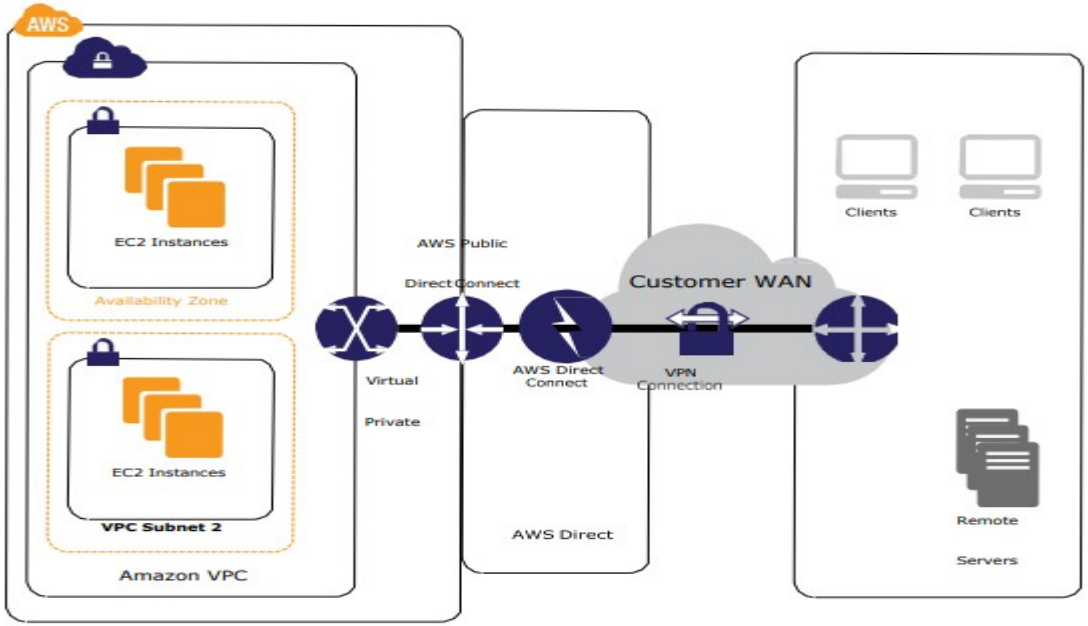
https://docs.aws.amazon.com/lambda/latest/dg/security-dataprotection.html

https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Security.html#CHAP_Security.IAMPermissions



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

Q-9



AWS Direct Connect and VPN

https://d1.awsstatic.com/whitepapers/aws-amazon-vpc-connectivity-options.pdf

Q-10

When a user performs a DELETE operation on an object, subsequent simple (un-versioned) requests will no longer retrieve the object. However, all versions of that object will continue to be preserved in your Amazon S3 bucket and can be retrieved or restored.

Versioning's MFA Delete capability, which uses multi-factor authentication, can be used to provide an additional layer of security. By default, all requests to your Amazon S3 bucket require your AWS account credentials. If you enable Versioning with MFA Delete on your Amazon S3 bucket, two forms of authentication are required to permanently delete a version of an object: your AWS account credentials and valid six-digit code and serial number from an authentication device in your physical possession.

For the root user, you should follow the best practice of using to create initial and another set of IAM users and groups for longer-term identity management

Monitoring and alerting for key metrics and events are the best practices of the Performance Efficiency pillar.

Non-overlapping Private IP addresses are in the Reliability pillar.

Designing with elasticity is in the Performance Efficiency pillar (Design for Cloud Operations).

Q-12

Regardless of whether you enable automated snapshots, you can take a manual snapshot whenever you want at any time. By default, manual snapshots are retained indefinitely, even after you delete your cluster. You can specify the retention period when you create a manual snapshot or change the retention period by modifying the snapshot.

To reduce cost, we can delete the manual snapshots that are taken, if any.

Backup storage is the storage associated with the snapshots taken for your data warehouse. Increasing your backup retention period or taking additional snapshots increases the backup storage consumed by your data warehouse.

- For example, if your RA3 cluster has 10 TB of data and 30 TB of manual snapshots, you would be billed for 10 TB of RMS and 30 TB of backup storage. With dense compute (DC) and dense storage (DS) clusters, storage is included on the cluster and is not billed separately, but backups are stored externally in Amazon S3. Backup storage beyond the provisioned storage size on DC and DS clusters is billed as backup storage at standard S3 rates. Snapshots are billed until they expire or are deleted, including when the cluster is paused or deleted.

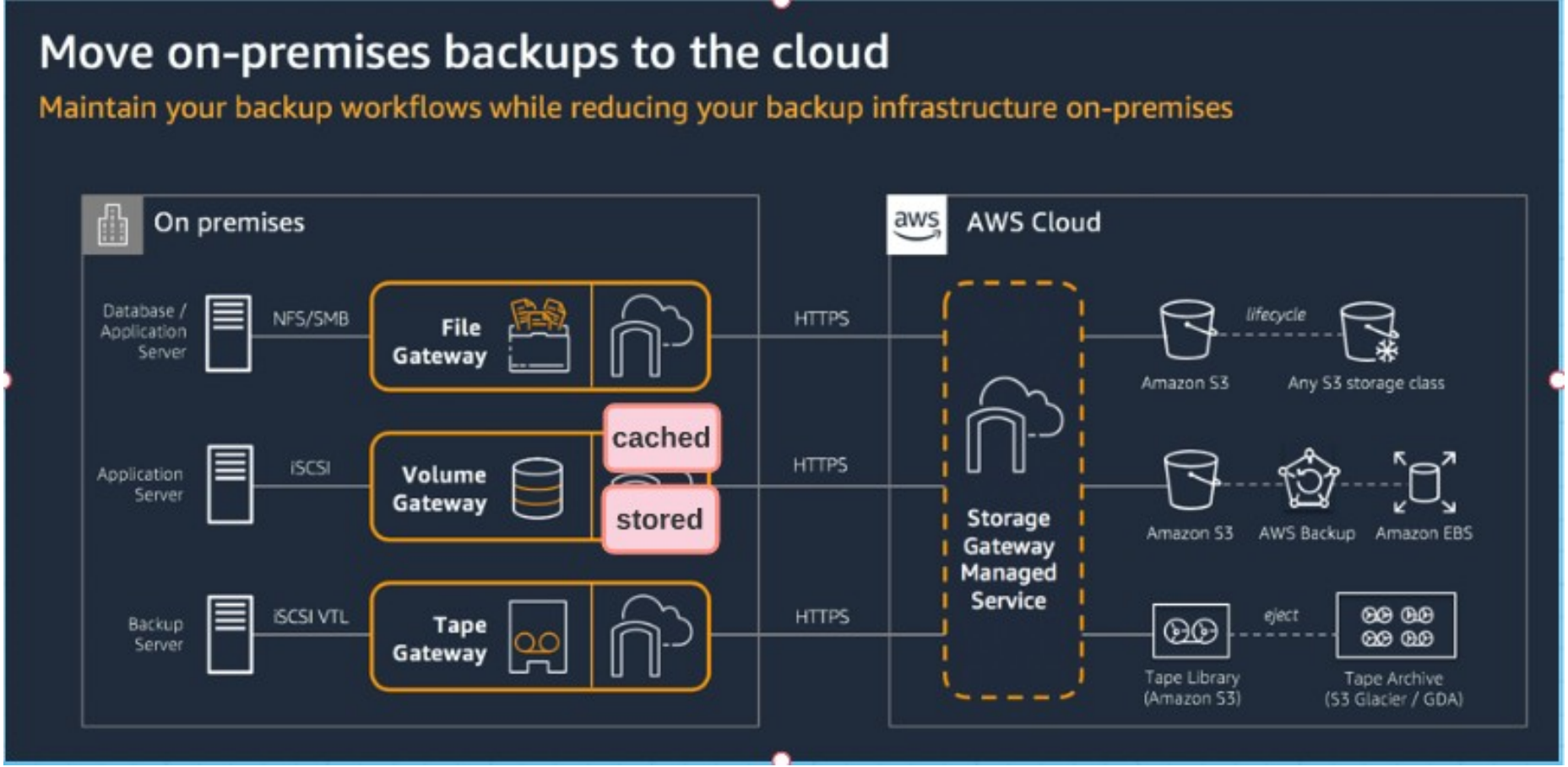
Automated snapshots are automatically deleted within the period of 1(Least) to **35(Max)** days (Based on the retention period settings). So we have to take care of the Manual snapshots instead of Automated snapshots. Amazon Redshift never deletes Manual snapshots automatically, as how it does for Automatic Snapshots.

Using the elastic load balancer to perform health checks will determine whether or not to remove a non-performing or underperforming instance, and have the auto-scaling group launch a new instance.

Increasing the instance size doesn't prevent the failure of one or both instances. Therefore the website can still become slow or unavailable.

Monitoring the VPC flow logs for the VPC will capture the VPC traffic, not the traffic for the EC2 instance. You would need to create a flow log for a network interface.

Replicating the same two instance deployment may not prevent instances of failure and could still result in the website becoming slow or unavailable.



Data on the volumes is stored in Amazon S3 and you can take point in time copies of volumes which are stored in AWS as Amazon EBS snapshots.

Q-15

Option B is CORRECT because both API Gateway/Lambda and Amazon DynamoDB are serverless, and hence the process of deploying servers is simplified.

Archive Retrieval Options

When initiating a job to retrieve an archive, you can specify one of the following retrieval options, based on your access time and cost requirements. For information about retrieval pricing, see Amazon S3 Glacier Pricing.

- **Expedited** – Expedited retrievals allow you to quickly access your data that's stored in the S3 Glacier Flexible Retrieval storage class or the S3 Intelligent-Tiering Archive Access tier when occasional urgent requests for a subset of archives are required. For all but the largest archives (more than 250 MB), data accessed by using Expedited retrievals is typically made available within 1–5 minutes. Provisioned capacity ensures that retrieval capacity for Expedited retrievals is available when you need it. For more information, see Provisioned Capacity.
- **Standard** – Standard retrievals allow you to access any of your archives within several hours. Standard retrievals are typically completed within 3–5 hours. This is the default option for retrieval requests that do not specify the retrieval option.
- **Bulk** – Bulk retrievals are the lowest-cost S3 Glacier retrieval option, which you can use to retrieve large amounts, even petabytes, of data inexpensively in a day. Bulk retrievals are typically completed within 5–12 hours.

Glacier Retrievals: Expedited and Bulk Retrievals

New

Clip slid

- Expedited: designed for occasional urgent access to a small number of archives
- Standard: Low-cost option for retrieving data in just a few hours
- Bulk: Lowest cost option optimized for large retrievals, up to petabytes of data in 12 hours
- Three flexible and powerful retrieval options to access any of your Glacier data

	Expedited	Standard	Bulk
Data Access Time	1 - 5 minutes	3 - 5 hours	5 - 12 hours
Data Retrievals	$0.03 per GB	$0.01 per GB	$0.0025 per GB
Retrieval Requests	$0.01 per request	$0.05 per 1,000 requests	$0.025 per 1,000 requests

aws

By configuring the frontend security group as the source, any frontend instances that have the specified security group are allowed to access the backend.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-security-groups.html#security-group-rules

Q-18

Option A is CORRECT. Compute Savings plans automatically apply to EC2 instance usage regardless of instance family, size, AZ, region, and OS. The web tier consists of multiple types of instance family. EC2 Instance Savings Plans automatically reduce cost on the selected instance family in that region regardless of AZ, size, OS, or tenancy.

Since application tiers use the same set of instance families. The savings plan doesn't support the RDS. So, Reserved instances are best suited for databases.

https://aws.amazon.com/savingsplans/faq/

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

ENI → ENA → EFA

- Upto 10 GBPS
- VMDq
- TCP/IP
- Multiple ENI/instance
- Traffic can traverse across subnets
- VPC Networking, General purpose
- Default

- Upto 25 GBPS
- SR-IOV
- TCP/IP
- Single setting/per instance
- Traffic can traverses across subnets
- Low latency apps
- Optional on supported instance type

- Upto 100 GBPS
- OS-Bypass
- SRD
- One EFA per instance
- OS Bypass traffic is limited to single subnet and is not routable
- HPC and ML Apps
- Optional on supported instance type

Q-21

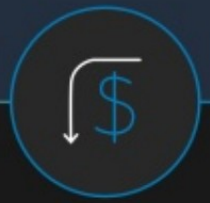
Amazon EMR

Easily Run Spark, Hadoop, Hive, Presto, HBase, and more big data apps on AWS

Latest versions

Updated with latest open source frameworks within 30 days

Low cost



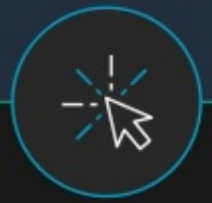
50–80% reduction in costs with EC2 Spot and Reserved Instances

Per-second billing for flexibility

Use S3 storage

Process data in S3 securely with high performance using the EMRFS connector

Easy



Fully managed no cluster setup, node provisioning, cluster tuning

S3 cross-region replication New

Automated, fast, and reliable asynchronous replication of data across AWS regions

Use cases

Compliance - store data hundreds of miles apart

Lower latency - distribute data to regional customers)

Security - create remote replicas managed by separate AWS accounts

- Only replicates new PUTs. Once S3 is configured, all new uploads into a source bucket will be replicated
- Entire bucket or prefix based
- 1:1 replication between any 2 regions
- Versioning required

Details on Cross-Region Replication

Versioning - Need to enable S3 versioning for the source and destination buckets.

Lifecycle Rules - You can choose to use Lifecyle Rules on the destination bucket to manage older versions by deleting them or migrating them to Amazon Glacier.

Determining Replication Status - Use the HEAD operation on a source object to determine its replication status.

Region-to-Region - Replication always takes place between a pair of AWS regions. You cannot use this feature to replicate content to two buckets that are in the same region.

New Objects - Replicates new objects and changes to existing objects. Use S3 COPY to replicate existing objects

Q-23

Object lifecycle management

Transition actions—Define when objects transition to another storage class

Expiration actions—Define when objects expire. Amazon S3 deletes expired objects on your behalf.

Trails

2

Delete | Create trail

Name	Home region	Multi-region trail	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
CloudTrail-event-log-files	US East (N. Virginia)	Yes	Disabled	No	aws-cloudtrail-logs-827784331229-b8c157f7			Logging

Trail name
Enter a display name for your trail.
CloudTrail event log files
3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

1

Enable for all accounts in my organization
To review accounts in your organization, open AWS Organizations. See all accounts

Storage location Info

- Create new S3 bucket
  Create a bucket to store logs for the trail.
- Use existing S3 bucket
  Choose an existing bucket to store logs for this trail.

Trail log bucket and folder
Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.
aws-cloudtrail-logs-827784331229-b8c157f7
Logs will be stored in aws-cloudtrail-logs-827784331229-b8c157f7/AWSLogs/827784331229

Log file SSE-KMS encryption Info
Enabled

AWS KMS customer managed CMK

- New
- Existing

AWS KMS alias
Enter KMS alias
KMS key and S3 bucket must be in the same region.

Additional settings

Log file validation Info
Enabled

Amazon S3 > aws-cloudtrail-logs-827784331229-b8c157f7 > AWSLogs/ > 827784331229/

827784331229/

3

Objects | Folder properties

Objects (2)

Objects are the fundamental entities stored in Amazon S3. For others to access your objects, you'll need to explicitly grant them permissions.

Delete | Actions | Create folder | Upload

Find objects by prefix

Name	Type	Last modified
CloudTrail-Digest/	Folder	-
CloudTrail/	Folder	-

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html

Different subnets for EC2 instances and transit gateway association

Consider a configuration where you have EC2 instances in one subnet and the transit gateway association in a different subnet, and each subnet is associated with a different network ACL.

Network ACL rules are applied as follows for the EC2 instance subnet:

- Outbound rules use the destination IP address to evaluate traffic from the instances to the transit gateway.
- Inbound rules use the source IP address to evaluate traffic from the transit gateway to the instances.

NACL rules are applied as follows for the transit gateway subnet:

- Outbound rules use the destination IP address to evaluate traffic from the transit gateway to the instances.
- Outbound rules are not used to evaluate traffic from the instances to the transit gateway.
- Inbound rules use the source IP address to evaluate traffic from the instances to the transit gateway.
- Inbound rules are not used to evaluate traffic from the transit gateway to the instances.

https://docs.aws.amazon.com/vpc/latest/tgw/tgw-nacls.html

Q-27

Amazon EC2 Auto Scaling lifecycle hooks

PDF | RSS

Amazon EC2 Auto Scaling offers the ability to add lifecycle hooks to your Auto Scaling groups. These hooks let you create solutions that are aware of events in the Auto Scaling instance lifecycle, and then perform a custom action on instances when the corresponding lifecycle event occurs. A lifecycle hook provides a specified amount of time (one hour by default) to wait for the action to complete before the instance transitions to the next state.

As an example of using lifecycle hooks with Auto Scaling instances:

- When a scale-out event occurs, your newly launched instance completes its startup sequence and transitions to a wait state. While the instance is in a wait state, it runs a script to download and install the needed software packages for your application, making sure that your instance is fully ready before it starts receiving traffic. When the script is finished installing software, it sends the **complete-lifecycle-action** command to continue.
- When a scale-in event occurs, a lifecycle hook pauses the instance before it is terminated and sends you a notification using Amazon EventBridge. While the instance is in the wait state, you can invoke an AWS Lambda function or connect to the instance to download logs or other data before the instance is fully terminated.

A popular use of lifecycle hooks is to control when instances are registered with Elastic Load Balancing. By adding a launch lifecycle hook to your Auto Scaling group, you can ensure that your bootstrap scripts have completed successfully and the applications on the instances are ready to accept traffic before they are registered to the load balancer at the end of the lifecycle hook.

https://docs.aws.amazon.com/autoscaling/ec2/userguide/lifecycle-hooks.html

Q-28

us-west-2 region

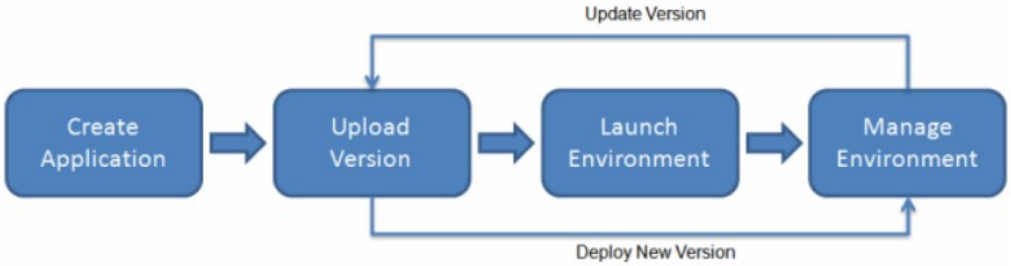
a	b	c	Total	
2	2	2	6	
3	3		6	
4	2	2	8	
6	6		12	
3	3	3	9	

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

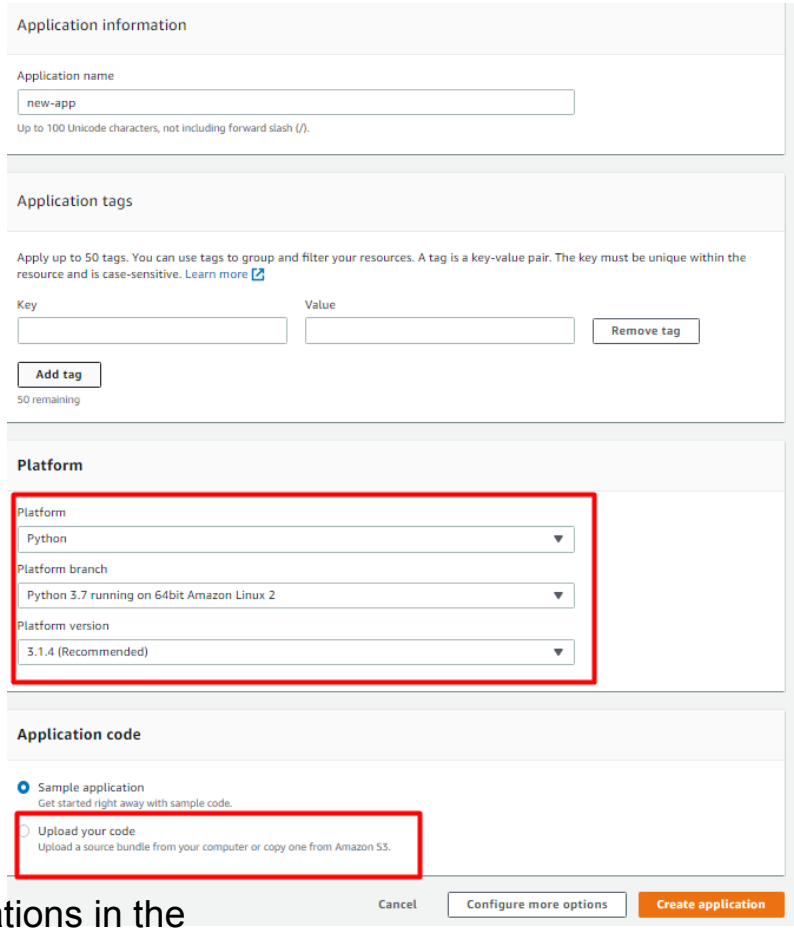
Option C is CORRECT because AWS Global Accelerator is a service that redirects users requests to the nearest edge location and then routes the data to the Amazon global network, increasing the speed and security of data transfer, therefore, increasing the performance of our applications. It also reroutes requests to healthy IPs if it fails and changes propagations. It is automatic and lasts some seconds.

Q: How is AWS Global Accelerator different from a DNS-based traffic management solution?

A: First, some client devices and internet resolvers cache DNS answers for long periods of time. So when you make a configuration update, or there's an application failure or change in your routing preference, you don't know how long it will take before all of your users receive updated IP addresses. With AWS Global Accelerator, you don't have to rely on the IP address caching settings of client devices. Change propagation takes a matter of seconds, which reduces your application downtime. Second, with Global Accelerator, you get static IP addresses that provide a fixed entry point to your applications. This lets you easily move your endpoints between Availability Zones or between AWS Regions, without having to update the DNS configuration or client-facing applications.



Java,
.NET,
PHP,
Node.js,
Python,
Ruby,
Go,
and Docker



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. (web tier – worker tier)

Q-32

Solid State Drives (SSD)						Hard Disk Drives (HDD)	
Volume Type	EBS Provisioned IOPS SSD (io2 Block Express)	EBS Provisioned IOPS SSD (io2)	EBS Provisioned IOPS SSD (io1)	EBS General Purpose SSD (gp3) **announced Dec 1, 2020**	EBS General Purpose SSD (gp2)*	Throughput Optimized HDD (st1)	Cold HDD (sc1)
Short Description	Highest performance SSD volume designed for business-critical latency-sensitive **transactional workloads**	**Highest performance** and highest durability SSD volume designed for **latency-sensitive transactional workloads**	Highest performance SSD volume designed for **latency-sensitive transactional workloads**	**Lowest cost SSD volume that balances price performance for a wide variety of transactional workloads**	General Purpose SSD volume that **balances price performance for a wide variety of transactional workloads**	**Low cost** HDD volume designed for **frequently** accessed, **throughput intensive workloads**	**Lowest cost** HDD volume designed for **less frequently accessed workloads**
Durability	99.999%		99.8% - 99.9% durability			99.8% - 99.9% durability	
Use Cases	Largest, most I/O intensive, mission critical deployments of NoSQL and relational **databases** such as Oracle, SAP HANA, Microsoft SQL Server, and SAS Analytics	I/O-intensive NoSQL and relational **databases**	I/O-intensive NoSQL and relational **databases**	Virtual desktops, medium sized single instance **databases** such as Microsoft SQL Server and Oracle, latency sensitive interactive applications, boot volumes, and dev/test environments	Virtual desktops, medium sized single instance **databases** such as Microsoft SQL Server and Oracle, latency sensitive interactive applications, boot volumes, and dev/test environments	**Big data, data warehouses, log processing**	**Colder data requiring fewer scans per day**

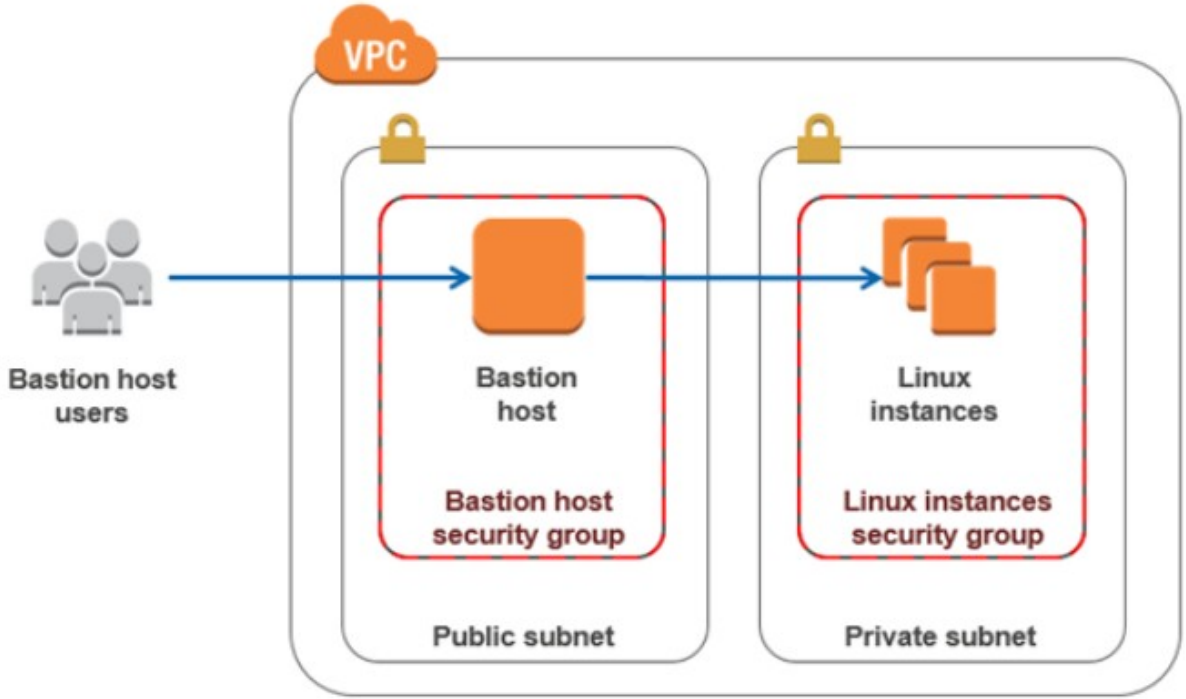
Q-33

Solid State Drives (SSD)						Hard Disk Drives (HDD)	
Volume Type	EBS Provisioned IOPS SSD (io2 Block Express)	EBS Provisioned IOPS SSD (io2)	EBS Provisioned IOPS SSD (io1)	EBS General Purpose SSD (gp3)	EBS General Purpose SSD (gp2)*	Throughput Optimized HDD (st1)	Cold HDD (sc1)
API Name	io2	io2	io1	gp3	gp2	st1	sc1
Volume Size	4 GB – 64 TB			1 GB - 16 TB		125 GB - 16 TB	
Max IOPS**/Volume	256,000	64,000	64,000	16,000	16,000	500	250
Max Throughput***/Volume	4,000 MB/s	1,000 MB/s	1,000 MB/s	1,000 MB/s	250 MB/s	500 MB/s	250 MB/s
Max IOPS/Instance	260,000	160,000**	260,000	260,000	260,000	260,000	260,000
Max Throughput/Instance	7,500 MB/s	4,750 MB/s**	7,500 MB/s	7,500 MB/s	7,500 MB/s	7,500 MB/s	7,500 MB/s
Latency	sub-millisecond	single digit millisecond					
Price	$0.125/GB-month $0.065/provisioned IOPS-month up to 32,000 IOPS $0.046/provisioned IOPS-month from 32,001 to 64,000 $0.032/provisioned IOPS-month for greater than 64,000 IOPS		$0.125/GB-month $0.065/provisioned IOPS-month	$0.08/GB-month 3,000 IOPS free and $0.005/provisioned IOPS-month over 3,000; 125 MB/s free and $0.04/provisioned MB/s-month over 125	$0.10/GB-month	$0.045/GB-month	$0.015/GB-month
Dominant Performance Attribute	IOPS, throughput, latency, capacity, and volume durability	IOPS and volume durability	IOPS	IOPS	IOPS	MB/s	MB/s

Q-33

https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-mixed-instances-groups.html#instances-distribution

Q-34


VPC
Bastion host users
Bastion host
Bastion host security group
Public subnet
Linux instances
Linux instances security group
Private subnet

Q-35

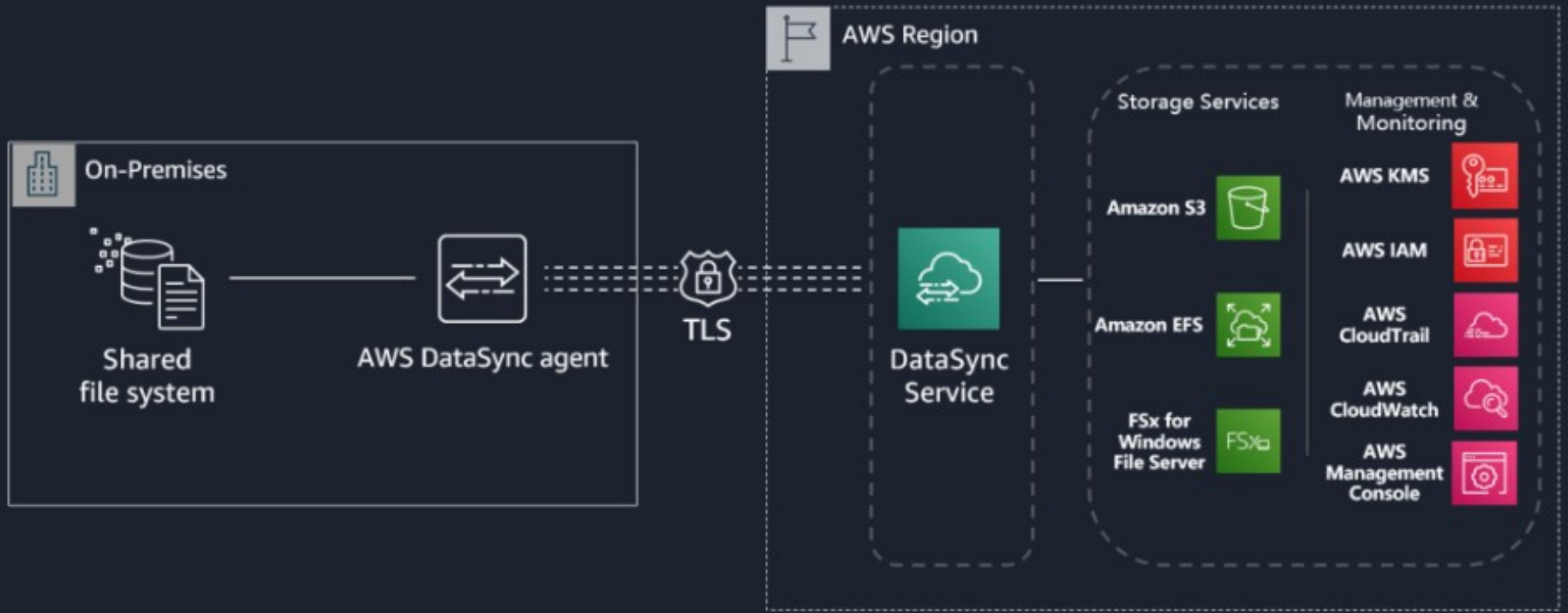
AWS CloudFormation Drift Detection can be used to detect changes made to AWS resources outside the CloudFormation Templates. AWS CloudFormation Drift Detection only checks property values explicitly set by stack templates or by specifying template parameters. It does not determine drift for property values that are set by default. To determine drift for these resources, you can explicitly set property values that can be the same as that of the default value.

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

Q-36

How does AWS DataSync work?

Simplifies, automates, and accelerates data transfer to or from AWS



https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html

https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global-accelerator.html

Object lifecycle management

Transition actions—Define when objects transition to another storage class

Expiration actions—Define when objects expire. Amazon S3 deletes expired objects on your behalf.

AWS CloudFormation enables consultants to use their architecture diagrams to construct CloudFormation templates.

AWS CloudFormation is a service that helps you model and set up your Amazon Web Service resources. You create a template that describes all the AWS resources that you want (like Amazon EC2 instances or Amazon RDS DB instances), and AWS CloudFormation takes care of provisioning and configuring those resources for you.

AWS Key Management Service (AWS KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data. AWS KMS is integrated with other AWS services including Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), Amazon Redshift, Amazon Elastic Transcoder, Amazon WorkMail, Amazon Relational Database Service (Amazon RDS), and others to make it simple to encrypt your data with encryption keys that you manage.

https://docs.aws.amazon.com/kms/latest/developerguide/overview.html

Q-42

Comparing the Amazon S3 storage classes

The following table compares the storage classes.

Storage class	Designed for	Durability (designed for)	Availability (designed for)	Availability Zones	Min storage duration
S3 Standard	Frequently accessed data	99.999999999%	99.99%	>= 3	None
S3 Standard-IA	Long-lived, infrequently accessed data	99.999999999%	99.9%	>= 3	30 days
S3 Intelligent-Tiering	Long-lived data with changing or unknown access patterns	99.999999999%	99.9%	>= 3	30 days
S3 One Zone-IA	Long-lived, infrequently accessed, non-critical data	99.999999999%	99.5%	1	30 days
S3 Glacier	Long-term data archiving with retrieval times ranging from minutes to hours	99.999999999%	99.99% (after you restore objects)	>= 3	90 days
S3 Glacier Deep Archive	Archiving rarely accessed data with a default retrieval time of 12 hours	99.999999999%	99.99% (after you restore objects)	>= 3	180 days
RRS (Not recommended)	Frequently accessed, non-critical data	99.99%	99.99%	>= 3	None

Q-43

Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale. It is a fully managed cloud database and supports both document and key-value store models. Its flexible data model, reliable performance, and automatic scaling of throughput capacity make it a great fit for mobile, web, gaming, ad tech, IoT, and many other applications.

AWS ElastiCache is a web service that makes it easy to set up, manage, and scale a distributed in-memory data store or cache environment in the cloud. It provides a high-performance, scalable, and cost-effective caching solution while removing the complexity associated with the deployment and management of a distributed cache environment.

Q-44

Aurora can have a storage limit of 64TB and can easily accommodate the initial 8TB plus a database growth of 8GB/day for nearly a period of 20+ years. It can have up to 15 Aurora Replicas that can be distributed across the Availability Zones that a DB cluster spans within an AWS Region.

Aurora Replicas work well for read scaling because they are fully dedicated to read operations on the cluster volume. Write operations are managed by the primary instance. Because the cluster volume is shared among all DB instances in your DB cluster, no additional work is required to replicate a copy of each Aurora Replica data.

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

Q-45

Option B is CORRECT. Clustered Placement Group places all the instances on the same rack. This placement group option provides 10 Gbps connectivity between instances (Internet connectivity in the instances has a maximum of 5 Gbps). This option of placement group is perfect for the workload that needs low latency. More details-

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

What is FSx for Windows File Server?

PDF | RSS

Amazon FSx for Windows File Server provides fully managed Microsoft Windows file servers, backed by a fully native Windows file system. FSx for Windows File Server has the features, performance, and compatibility to easily lift and shift enterprise applications to the AWS Cloud.

Amazon FSx supports a broad set of enterprise Windows workloads with fully managed file storage built on Microsoft Windows Server. Amazon FSx has native support for Windows file system features and for the industry-standard Server Message Block (SMB) protocol to access file storage over a network. Amazon FSx is optimized for enterprise applications in the AWS Cloud, with native Windows compatibility, enterprise performance and features, and consistent sub-millisecond latencies.

With file storage on Amazon FSx, the code, applications, and tools that Windows developers and administrators use today can continue to work unchanged. Windows applications and workloads ideal for Amazon FSx include business applications, home directories, web serving, content management, data analytics, software build setups, and media processing workloads.

As a fully managed service, FSx for Windows File Server eliminates the administrative overhead of setting up and provisioning file servers and storage volumes.

Logging IP traffic using VPC Flow Logs

PDF | RSS

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to the following locations: Amazon CloudWatch Logs, Amazon S3, or Amazon Kinesis Data Firehose. After you create a flow log, you can retrieve and view the flow log records in the log group, bucket, or delivery stream that you configured.

Flow logs can help you with a number of tasks, such as:

- Diagnosing overly restrictive security group rules
- Monitoring the traffic that is reaching your instance
- Determining the direction of the traffic to and from the network interfaces

Flow log data is collected outside of the path of your network traffic, and therefore does not affect network throughput or latency. You can create or delete flow logs without any risk of impact to network performance.

Q-48

AWS Organizations helps you centrally govern your environment as you scale your workloads on AWS. Whether you are a growing startup or a large enterprise, Organizations helps you to programmatically create new accounts and allocate resources, simplify billing by setting up a single payment method for all of your accounts, create groups of accounts to organize your workflows, and apply policies to these groups for governance. In addition, AWS Organizations is integrated with other AWS services so you can define central configurations, security mechanisms, and resource sharing across accounts in your organization.

AWS Organizations enables the following capabilities:

- Automate AWS account creation and management, and provision resources with AWS CloudFormation Stacksets
- Maintain a secure environment with policies and management of AWS security services
- Govern access to AWS services, resources, and regions
- Centrally manage policies across multiple AWS accounts
- Audit your environment for compliance
- View and manage costs with consolidated billing
- Configure AWS services across multiple accounts

Q-49


Amazon FSx for Lustre
Create
Create your file system using the AWS Management Console, CLI, or SDK
Link to Amazon S3 (Optional)
Link your file system to your Amazon S3 bucket to access and process your S3 datasets
Amazon EC2
Amazon ECS & EKS
On-premises clients
Access
Access your file system from Linux clients in AWS, or on premises
Amazon SageMaker
AWS ParallelCluster & AWS Batch
Nimble Studio
Run
Run your ML, HPC, and media rendering applications with high performance shared storage

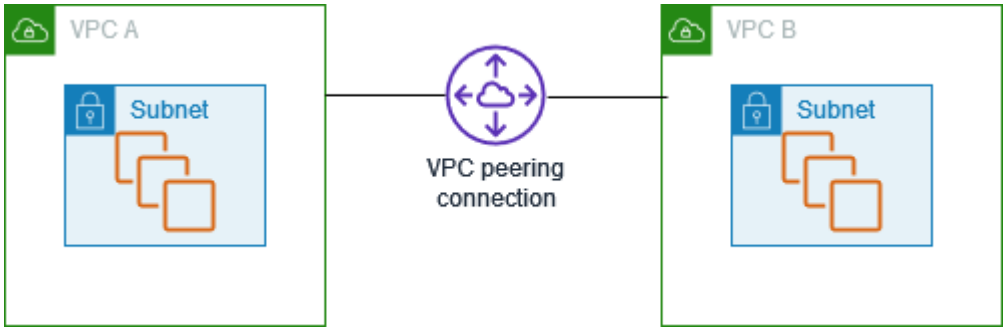
- A gateway endpoint is available only in the Region where you created it. Be sure to create your gateway endpoint in the same Region as your S3 buckets.
- If you're using the Amazon DNS servers, you must enable both DNS hostnames and DNS resolution for your VPC. If you're using your own DNS server, ensure that requests to Amazon S3 resolve correctly to the IP addresses maintained by AWS.
- Check whether you are using an AWS service that requires access to an S3 bucket. For example, a service might require access to buckets that contain log files, or might require you to download drivers or agents to your EC2 instances. If so, ensure that your endpoint policy allows the AWS service or resource to access these buckets using the `s3:GetObject` action.
- You cannot use an IAM policy or bucket policy to allow access from an VPC IPv4 CIDR range. VPC CIDR blocks can be overlapping or identical, which might lead to unexpected results. Therefore, you can't use the `aws:SourceIp` condition in your IAM policies for requests to Amazon S3 through a VPC endpoint. This applies to IAM policies for users and roles, and to any bucket policies. If a statement includes the `aws:SourceIp` condition, the value fails to match any provided IP address or range. Instead, you can do the following:
  - Use route tables to control which instances can access resources in Amazon S3 through the gateway endpoint.
  - Use bucket policies to restrict access to a specific endpoint, VPC, or IP address range.
- The outbound rules for the security group for instances that access Amazon S3 through the gateway endpoint must allow traffic to Amazon S3. You can use the prefix list ID for Amazon S3 as the destination in the outbound rule.
- Gateway endpoints support only IPv4 traffic.
- The source IPv4 addresses from instances in your affected subnets as received by Amazon S3 change from public IPv4 addresses to the private IPv4 addresses in your VPC. An endpoint switches network routes, and disconnects open TCP connections. The previous connections that used public IPv4 addresses are not resumed. We recommend that you do not have any critical tasks running when you create or modify an endpoint; or that you test to ensure that your software can automatically reconnect to Amazon S3 after the connection break.
- Endpoint connections cannot be extended out of a VPC. Resources on the other side of a VPN connection, VPC peering connection, transit gateway, or AWS Direct Connect connection in your VPC cannot use a gateway endpoint to communicate with Amazon S3.
- Your account has a default quota of 20 gateway endpoints per Region, which is adjustable. There is also a limit of 255 gateway endpoints per VPC.

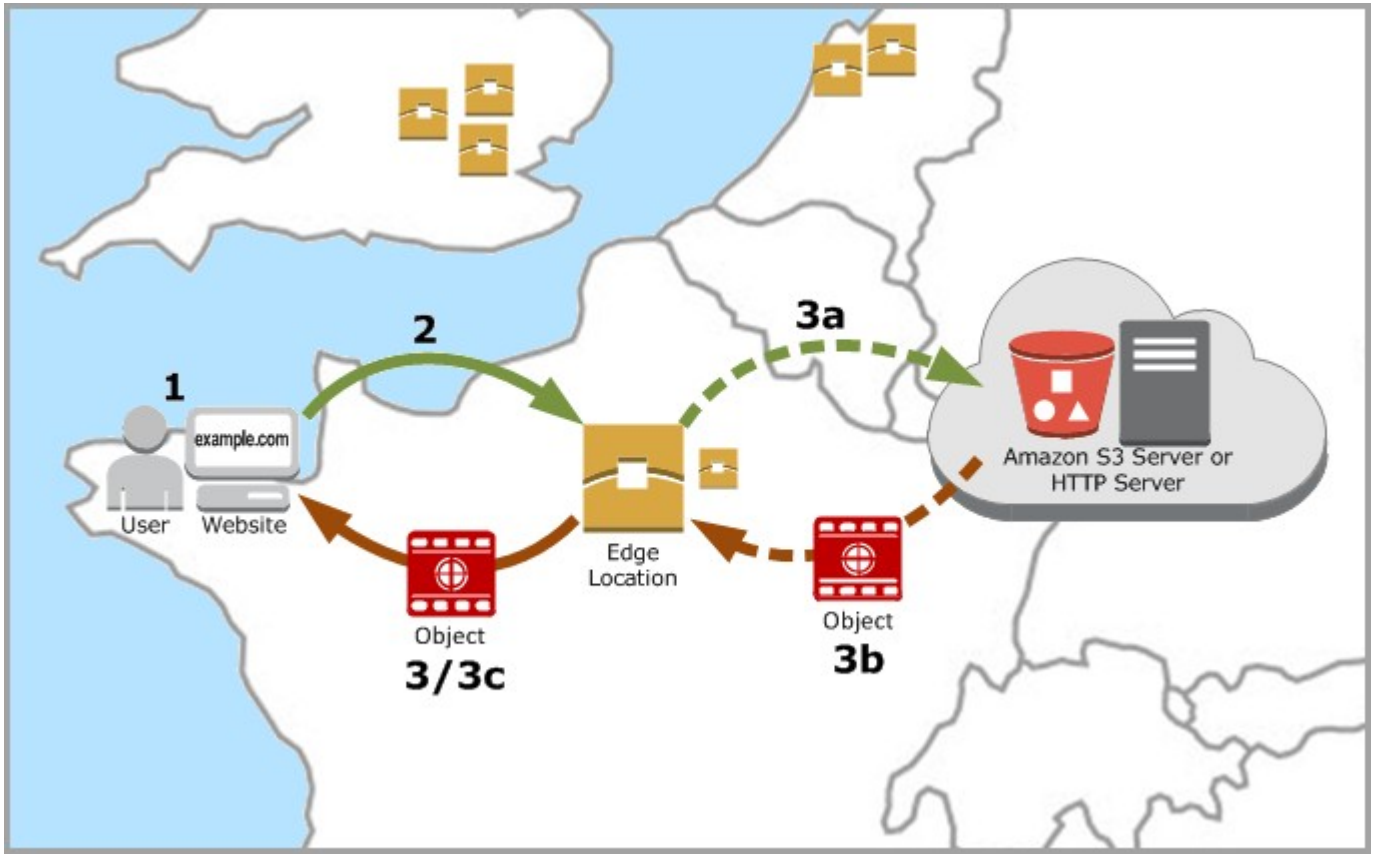
Connect VPCs using VPC peering

PDF | RSS

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, with a VPC in another AWS account, or with a VPC in a different AWS Region.

AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor an AWS Site-to-Site VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.





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

Q-53

Since there is only one NAT Gateway, this is a bottleneck in the architecture. For high availability, launch NAT Gateways in multiple Available Zones.

If you have resources in multiple Availability Zones and they share one NAT gateway, and if the NAT gateway's Availability Zone is down, resources in the other Availability Zones lose internet access. To create an Availability Zone-independent architecture, create a NAT gateway in each Availability Zone and configure your routing to ensure that resources use the NAT gateway in the same Availability Zone.

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html#nat-gateway-basics

- Manual Scaling **- Dynamic Scaling** **- Predictive Scaling** **- Scheduled Scaling**

- **Target tracking scaling**—Increase and decrease the current capacity of the group based on a Amazon CloudWatch metric and a target value. It works similar to the way that your thermostat maintains the temperature of your home—you select a temperature and the thermostat does the rest.
- **Step scaling**—Increase and decrease the current capacity of the group based on a set of scaling adjustments, known as *step adjustments*, that vary based on the size of the alarm breach.
- **Simple scaling**—Increase and decrease the current capacity of the group based on a single scaling adjustment, with a cooldown period between each scaling activity.

If you are scaling based on a metric that increases or decreases proportionally to the number of instances in an Auto Scaling group, we recommend that you use target tracking scaling policies. Otherwise, we recommend that you use step scaling policies.

With target tracking, an Auto Scaling group scales in direct proportion to the actual load on your application. That means that in addition to meeting the immediate need for capacity in response to load changes, a target tracking policy can also adapt to load changes that take place over time, for example, due to seasonal variations.

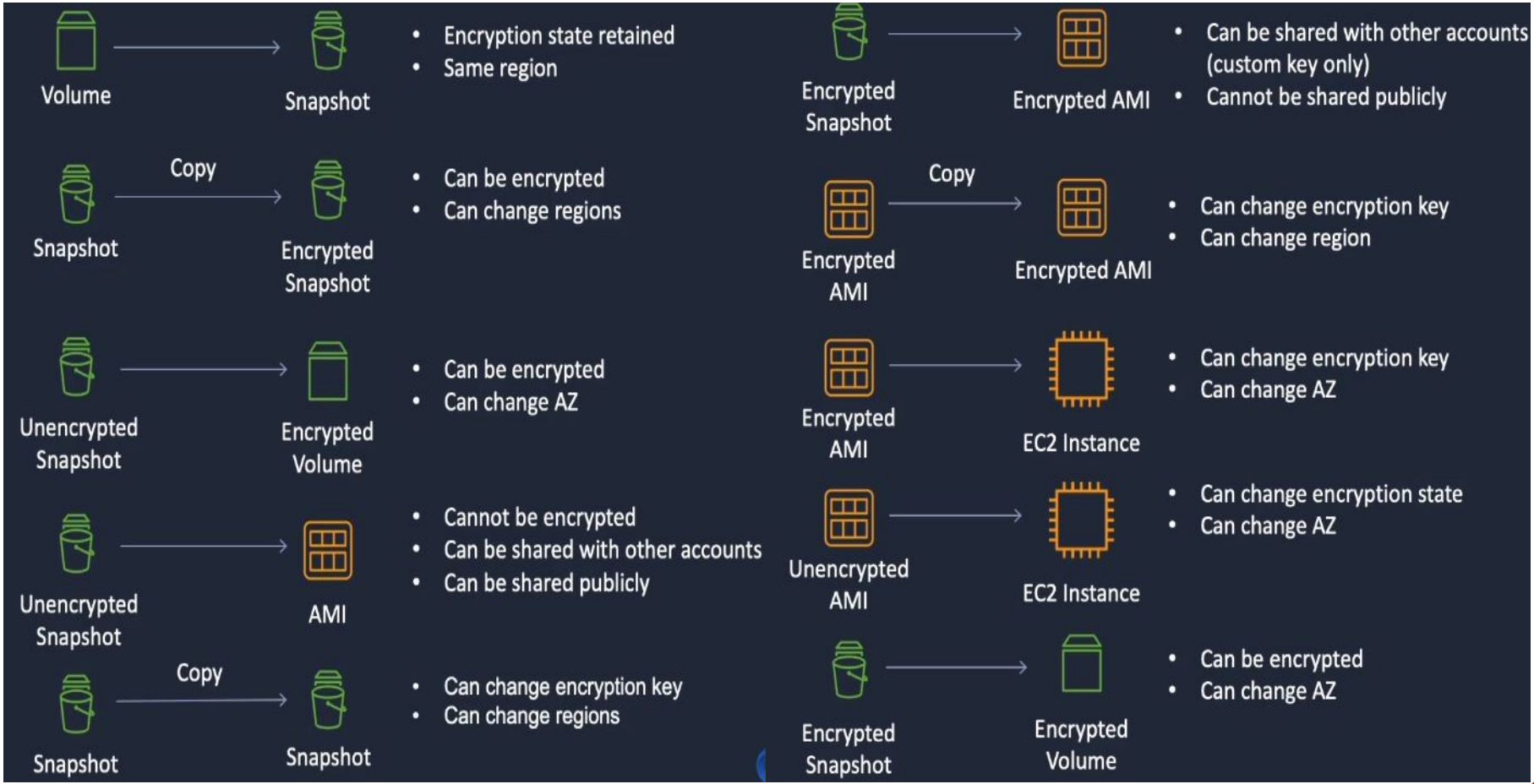
Q-55

- Manual Scaling - Dynamic Scaling - Predictive Scaling - **Scheduled Scaling**

Scheduled scaling helps you to set up your own scaling schedule according to predictable load changes. For example, let's say that every week the traffic to your web application starts to increase on Wednesday, remains high on Thursday, and starts to decrease on Friday. You can configure a schedule for Amazon EC2 Auto Scaling to increase capacity on Wednesday and decrease capacity on Friday.

To use scheduled scaling, you create *scheduled actions*. Scheduled actions are performed automatically as a function of date and time. When you create a scheduled action, you specify when the scaling activity should occur and the new desired, minimum, and maximum sizes for the scaling action. You can create scheduled actions that scale one time only or that scale on a recurring schedule.

Q-56


Volume
Snapshot
• Encryption state retained
• Same region
Snapshot
Copy
Encrypted Snapshot
• Can be encrypted
• Can change regions
Unencrypted Snapshot
Encrypted Volume
• Can be encrypted
• Can change AZ
Unencrypted Snapshot
AMI
• Cannot be encrypted
• Can be shared with other accounts
• Can be shared publicly
Snapshot
Copy
Snapshot
• Can change encryption key
• Can change regions
Encrypted Snapshot
Encrypted AMI
• Can be shared with other accounts (custom key only)
• Cannot be shared publicly
Encrypted AMI
Copy
Encrypted AMI
• Can change encryption key
• Can change region
Encrypted AMI
EC2 Instance
• Can change encryption key
• Can change AZ
Unencrypted AMI
EC2 Instance
• Can change encryption state
• Can change AZ
Encrypted Snapshot
Encrypted Volume
• Can be encrypted
• Can change AZ

Q-57

https://docs.aws.amazon.com/awscloudtrail/latest/APIReference/Welcome.html

https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-cloudwatch-metrics.html

What is AWS Resource Access Manager?

PDF | RSS

AWS Resource Access Manager (AWS RAM) helps you securely share the AWS resources that you create in one AWS account with other AWS accounts. If you have multiple AWS accounts, you can create a resource once and use AWS RAM to make that resource usable by those other accounts. If your account is managed by AWS Organizations, then you can share resources with all the other accounts in the organization, or only those accounts contained by one or more specified organizational units (OUs). You can also share with specific AWS accounts by account ID, regardless of whether the account is part of an organization. Some supported resource types also let you share them with specified IAM roles and users.

https://docs.aws.amazon.com/ram/latest/userguide/shareable.html#shareable-ec2

Q-59

In a disaster recovery scenario, the best choice out of all given options is to divert the traffic to a static website.

Most organizations try to implement High Availability (HA) instead of DR to guard them against any downtime of services. In the case of HA, we ensure that there exists a fallback mechanism for our services. The service that runs in HA is handled by hosts running in different availability zones but the same geographical region. However, this approach does not guarantee that our business will be up and running in case the entire region goes down.

DR takes things to a completely new level, wherein you need to recover from a different region that is separated by over 250 miles. Our DR implementation is an Active/Passive model, meaning that we always have minimum critical services running in different regions. But a major part of the infrastructure is launched and restored when required.

Internet-scale applications

Real-time apps in Gaming, Ride Hailing, Media Streaming, Dating, and Social media need fast data access

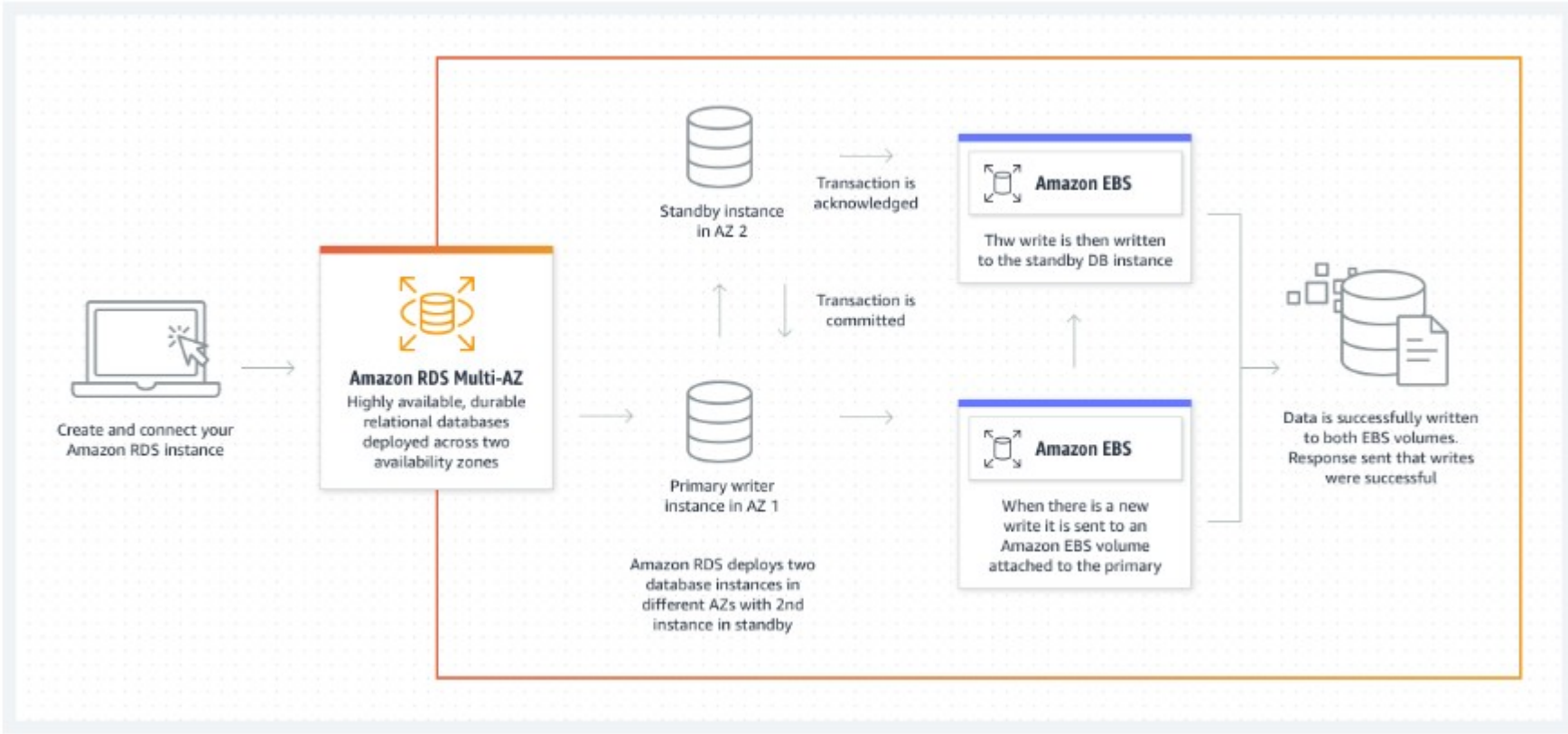
Amazon ElastiCache

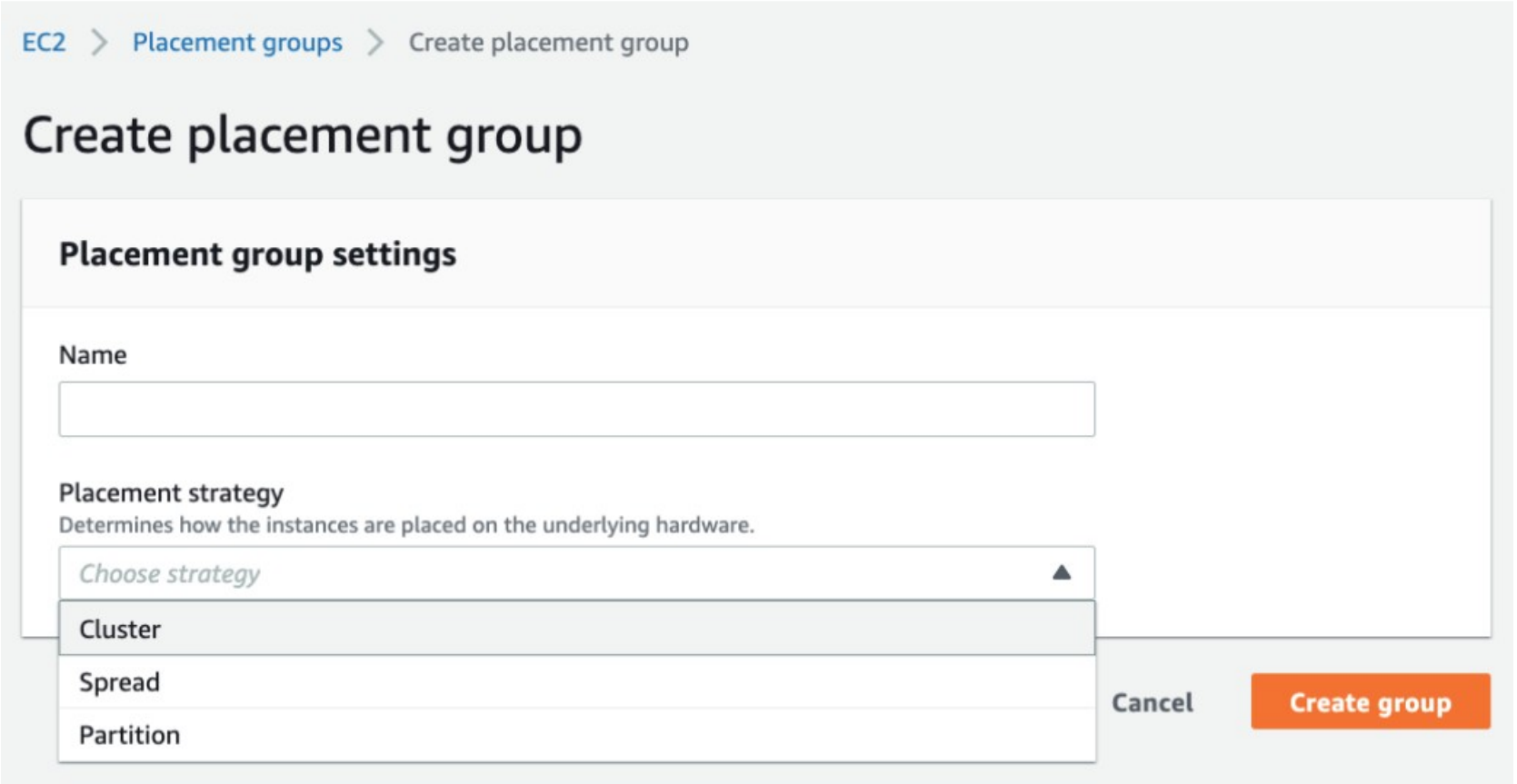
Blazing fast in-memory data store for use as a database, cache, message broker, and queue. Store ephemeral data in-memory for sub-millisecond response

Use cases

Real-time transactions, chat, BI and analytics, session store, gaming leaderboards, and cache

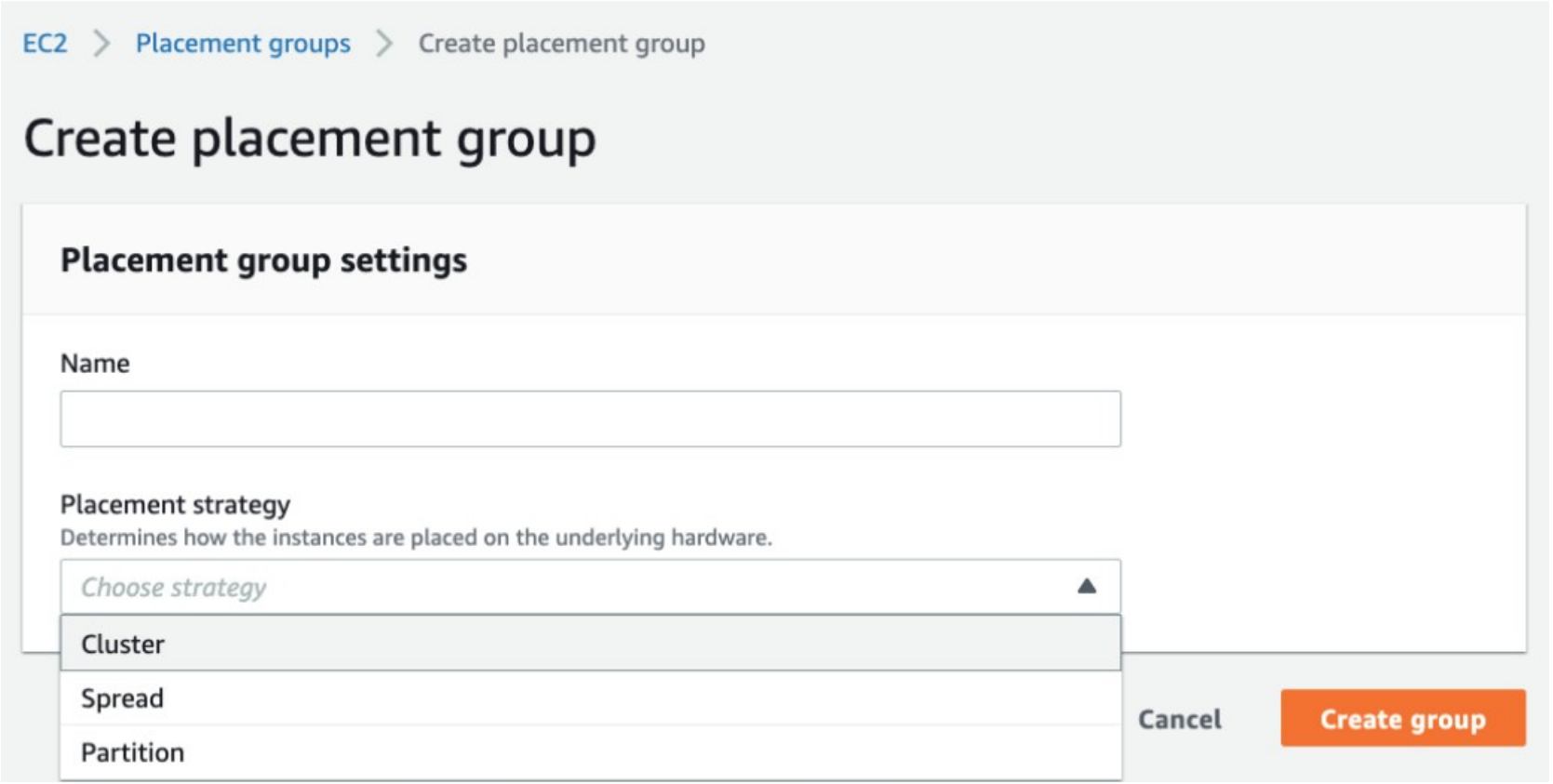
Q-61


Create and connect your Amazon RDS instance
Amazon RDS Multi-AZ
Highly available, durable relational databases deployed across two availability zones
Standby instance in AZ 2
Transaction is acknowledged
Transaction is committed
Primary writer instance in AZ 1
Amazon RDS deploys two database instances in different AZs with 2nd instance in standby
Amazon EBS
Thw write is then written to the standby DB instance
Amazon EBS
When there is a new write it is sent to an Amazon EBS volume attached to the primary
Data is successfully written to both EBS volumes. Response sent that writes were successful



Placement groups have the placement strategies of Cluster, Partition, and Spread. With the Partition placement strategy, instances in one partition do not share the underlying hardware with other partitions. This strategy is suitable for distributed and replicated workloads such as Cassandra.

Q-63



Cluster placement groups are recommended for applications that benefit from low network latency, high network throughput, or both. They are also recommended when the majority of the network traffic is between the instances in the group. To provide the lowest latency and the highest packet-per-second network performance for your placement group, choose an instance type that supports enhanced networking. For more information, see Enhanced Networking.

Q-64

Simple routing policy – basic routing policy defined using an A record to resolve to a single resource always without any specific rules.

Multivalue answer routing policy – Use when you want Route 53 to respond to DNS queries with up to eight healthy records selected at **random**.

Latency routing policy – is used when there are multiple resources (multiple AWS Regions) for the same functionality and you want Route 53 to respond to DNS queries with answers that provide the best latency.

Weighted routing policy – is good for testing new versions of the software. Also, It is the ideal approach for **Blue-Green** deployments.