Practice exams (Solutions Architect Associate)

Practice Set 2

- The solution must use NFS file shares to access the migrated data without code modification. This means you can use either Amazon EFS or AWS Storage Gateway – File Gateway. Both of these can be mounted using NFS from on-premises applications.
  However, EFS is the wrong answer as the solution asks to maximize availability and durability. The File Gateway backs off of Amazon S3 which has much higher availability and durability than EFS which is why it is the best solution for this scenario.
- DynamoDB offers consistent single-digit millisecond latency. However, DynamoDB + DAX further increases performance with response times in microseconds for millions of requests per second for read-heavy workloads.
- If you do not want to manage EC2 instances you must use the AWS Fargate launch type which is a serverless infrastructure managed by AWS. Fargate only supports container images hosted on Elastic Container Registry (ECR) or Docker Hub.
- Amazon EFS is a fully-managed service that makes it easy to set up, scale, and cost-optimize file storage in the Amazon Cloud. EFS file systems are accessible to Amazon EC2 instances via a file system interface (using standard operating system file I/O APIs) and support full file system access semantics (such as strong consistency and file locking).
- The most cost-effective option is to migrate the website to an Amazon S3 bucket and configure that bucket for static website hosting.
- Amazon S3 is great solution for storing objects such as this. You only pay for what you use and don't need to worry about scaling as it will scale as much as you need it to. Using Amazon Athena to analyze the data works well as it is a serverless service so it will be very cost-effective for use cases where the analysis is only happening infrequently. You can also configure Amazon S3 to expire the objects after 30 days.
- The ELB Application Load Balancer can route traffic based on data included in the request including the host name portion of the URL as well as the path in the URL.

- An application running on Amazon EC2 needs to regularly download large objects from Amazon S3. How can performance be optimized for high-throughput use cases?
    - Issue parallel requests and use byte-range fetches
- A mobile client requires data from several application-layer services to populate its user interface. What can the application team use to decouple the client interface from the underlying services behind them?
    - Amazon API Gateway decouples the client application from the back-end application-layer services by providing a single endpoint for API requests.
- Using Amazon CloudFront as the front-end provides the option to specify a custom message instead of the default message.
- ElastiCache can be deployed in the U.S east region to provide high-speed access to the content.
- AWS Global Accelerator is a service that improves the availability and performance of applications with local or global users. You can configure the ALB as a target and Global Accelerator will automatically route users to the closest point of presence.
- You can only apply one IAM role to a Task Definition so you must create a separate Task Definition. A Task Definition is required to run Docker containers in Amazon ECS and you can specify the IAM role (Task Role) that the task should use for permissions.
- That restrict access so that consumers cannot connect to other instances in the VPC the best solution is to use PrivateLink to create an endpoint for the application. The endpoint type will be an interface endpoint and it uses an NLB in the shared services VPC.
- You can encrypt your Amazon RDS instances and snapshots at rest by enabling the encryption option for your Amazon RDS DB instance when you create it. However, you cannot encrypt an existing DB, you need to create a snapshot, copy it, encrypt the copy, then build an encrypted DB from the snapshot.
- To publish messages to Amazon SNS topics from an Amazon VPC, create an interface VPC endpoint. Then, you can publish messages to SNS topics while keeping the traffic within the network that you manage with the VPC. This is the most secure option as traffic does not need to traverse the Internet.
    - AWS PrivateLink - is the correct answer.

- EC2 Instance Stores are high-speed ephemeral storage that is physically attached to the EC2 instance. The i3.large instance type comes with a single 475GB NVMe SSD instance store so it would be a good way to lower cost and improve performance by using the attached instance store. As the files are temporary, it can be assumed that ephemeral storage (which means the data is lost when the instance is stopped) is sufficient.
- The Amazon Elastic File System (EFS) can assist with increasing the resilience of the application by providing a shared file system that can be mounted by multiple EC2 instances from multiple availability zones.
- AWS Lambda can likewise be used for the back-end processing reducing cost by utilizing a pay for what you use serverless service.
- RedShift is a columnar data warehouse DB that is ideal for running long complex queries. RedShift can also improve performance for repeat queries by caching the result and returning the cached result when queries are re-run. Dashboard, visualization, and business intelligence (BI) tools that execute repeat queries see a significant boost in performance due to result caching.
- You have created a file system using Amazon Elastic File System (EFS) which will hold home directories for users. What else needs to be done to enable users to save files to the EFS file system?
    - Create a subdirectory for each user and grant read-write-execute permissions to the users. Then mount the subdirectory to the users' home directory.
- Amazon FSx for Windows File Server provides fully managed, highly reliable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol. It is built on Windows Server, delivering a wide range of administrative features such as user quotas, end-user file restore, and Microsoft Active Directory (AD) integration. It offers single-AZ and multi-AZ deployment options, fully managed backups, and encryption of data at rest and in transit.
- Which set of actions will improve website performance for users worldwide?
    - Create an Amazon CloudFront distribution and configure the ALB as an origin. Then update the Amazon Route 53 record to point to the CloudFront distribution.
- IAM roles for ECS tasks enabled you to secure your infrastructure by assigning an IAM role directly to the ECS task rather than to the EC2 container instance. This means you can have one task that uses a specific IAM role for access to S3 and one task that uses an IAM role to access DynamoDB.

- EBS volumes cannot be shared across AZs.
- Amazon FSx for Lustre provides a high-performance file system optimized for fast processing of workloads such as machine learning, high-performance computing (HPC), video processing, financial modeling, and electronic design automation (EDA).
- These workloads commonly require data to be presented via a fast and scalable file system interface, and typically have data sets stored on long-term data stores like Amazon S3.
- The microservices must be decoupled so they can scale independently. An Amazon SQS queue will enable microservice 1 to add messages to the queue. Microservice 2 can then pick up the messages and process them. This ensures that if there's a spike in traffic on the frontend, messages do not get lost due to the backend process not being ready to process them.
- The AWS Web Application Firewall (WAF) is available on the Application Load Balancer (ALB). You can use AWS WAF directly on Application Load Balancers (both internal and external) in a VPC, to protect your websites and web services from cross-site scripting (XSS) attacks.
- Amazon EFS provides file storage in the AWS Cloud. With Amazon EFS, you can create a file system, mount the file system on an Amazon EC2 instance, and then read and write data to and from your file system. Can be shared between multiple EC2 instances.
- Uploading using a pre-signed URL allows you to upload the object without having any AWS security credentials/permissions. Pre-signed URLs can be generated programmatically and anyone who receives a valid pre-signed URL can then programmatically upload an object. This solution bypasses the web server avoiding any performance bottlenecks.
- AWS Global Accelerator is a service in which you create accelerators to improve availability and performance of your applications for local and global users.
- The key requirements are that the compute service should be suitable for a workload that can range quite broadly in demand from no requests to large bursts of traffic.
  AWS Lambda is an ideal solution as you pay only when requests are made and it can easily scale to accommodate the large bursts in traffic. Lambda works well with both API Gateway and Amazon RDS.

- You can enable API caching in Amazon API Gateway to cache your endpoint's responses. With caching, you can reduce the number of calls made to your endpoint and also improve the latency of requests to your API.
  Когда вы включаете кэширование для этапа, API Gateway кэширует ответы от вашей конечной точки в течение указанного периода времени жизни (TTL), в секундах. Затем API Gateway отвечает на запрос, просматривая ответ конечной точки из кэша, вместо того чтобы делать запрос к вашей конечной точке. Значение TTL по умолчанию для кэширования API составляет 300 секунд. Максимальное значение TTL составляет 3600 секунд. TTL=0 означает, что кэширование отключено.

Practice Set 3

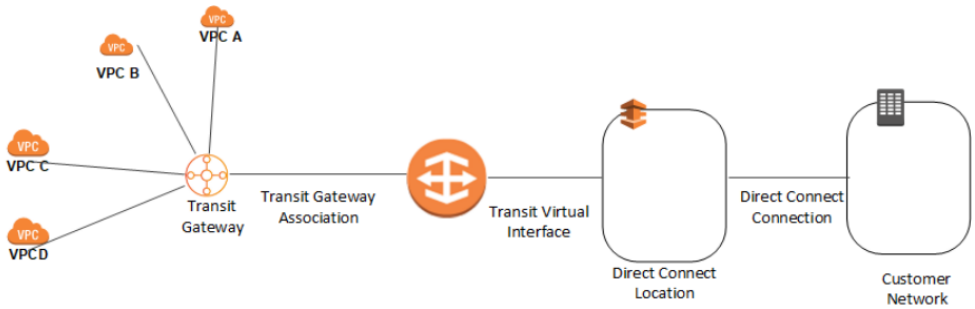
- Expedited — Expedited retrievals allow you to quickly access your data when occasional urgent requests for a subset of archives are required. For all but the largest archives (250 MB+), data accessed using Expedited retrievals are typically made available within 1–5 minutes. Provisioned Capacity ensures that retrieval capacity for Expedited retrievals is available when you need it.
- Standard — Standard retrievals allow you to access any of your archives within several hours. Standard retrievals typically complete within 3–5 hours. This is the default option for retrieval requests that do not specify the retrieval option.
- Bulk — Bulk retrievals are S3 Glacier's lowest-cost retrieval option, which you can use to retrieve large amounts, even petabytes, of data inexpensively in a day. Bulk retrievals typically complete within 5–12 hours.
- A VPG is used to setup an AWS VPN which you can use in combination with Direct Connect to encrypt all data that traverses the Direct Connect link.
- With target tracking scaling policies, you select a scaling metric and set a target value.

- Amazon Aurora Global Database is designed for globally distributed applications, allowing a single Amazon Aurora database to span multiple AWS regions. It replicates your data with no impact on database performance, enables fast local reads with low latency in each region, and provides disaster recovery from region-wide outages.
  Aurora Global Database uses storage-based replication with typical latency of less than 1 second, using dedicated infrastructure that leaves your database fully available to serve application workloads. In the unlikely event of a regional degradation or outage, one of the secondary regions can be promoted to full read/write capabilities in less than 1 minute.
- Amazon Simple Workflow Service (SWF) is a web service that makes it easy to coordinate work across distributed application components.
- The following are a few reasons why an instance might immediately terminate:
  – You've reached your EBS volume limit.
  – An EBS snapshot is corrupt.
  – The root EBS volume is encrypted and you do not have permissions to access the KMS key for decryption.
  – The instance store-backed AMI that you used to launch the instance is missing a required part (an image.part.xx file).
- You can use a Lambda function to process Amazon Simple Notification Service notifications. Amazon SNS supports Lambda functions as a target for messages sent to a topic. This solution decouples the Amazon EC2 application from Lambda and ensures the Lambda function is invoked.
- Multi-AZ RDS creates a replica in another AZ and synchronously replicates to it (DR only).
- A failover may be triggered in the following circumstances:
  – Loss of primary AZ or primary DB instance failure
  – Loss of network connectivity on primary
  – Compute (EC2) unit failure on primary
  – Storage (EBS) unit failure on primary
  – The primary DB instance is changed
  – Patching of the OS on the primary DB instance
  – Manual failover (reboot with failover selected on primary)

Practice Set 4

- To allow read access to the S3 video assets from the public-facing web application, you can add a bucket policy that allows s3:GetObject permission with a condition, using the aws:referer key, that the get request must originate from specific webpages. This is a good answer as it fully satisfies the objective of ensuring the that EC2 instance can access the videos but direct access to the videos from other sources is prevented.
- Многоузловые параллельные задания AWS Batch позволяют выполнять отдельные задания, охватывающие несколько экземпляров Amazon EC2. С помощью многоузловых параллельных заданий AWS Batch вы можете запускать крупномасштабные, тесно связанные, высокопроизводительные вычислительные приложения и распределенное обучение моделей на GPU без необходимости запуска, настройки и управления ресурсами Amazon EC2 напрямую.
  Многоузловое параллельное задание AWS Batch совместимо с любым фреймворком, поддерживающим межузловое взаимодействие на основе IP, например Apache MXNet, TensorFlow, Caffe2 или Message Passing Interface (MPI).
- Токены аутентификации Redis позволяют Redis запрашивать токен (пароль), прежде чем разрешить клиентам выполнять команды, что повышает безопасность данных.
  Вы можете потребовать, чтобы пользователи вводили токен на защищенном токенами сервере Redis. Для этого при создании группы репликации или кластера включите параметр -auth-token (API: AuthToken) с правильным маркером. Также включайте его во все последующие команды для группы или кластера репликации.
- сценарий требует использования учетных данных для аутентификации в MySQL. Учетные данные должны надежно храниться вне кода функции Lambda. Systems Manager Parameter Store обеспечивает безопасное, иерархическое хранение для управления конфигурационными данными и секретами.
- Без включенной межзональной балансировки нагрузки NLB будет распределять трафик 50/50 между AZ. Поскольку количество экземпляров в двух AZ нечетное, некоторые экземпляры не будут получать трафик. Поэтому включение межзональной балансировки нагрузки обеспечит равномерное распределение трафика между доступными экземплярами во всех AZ.

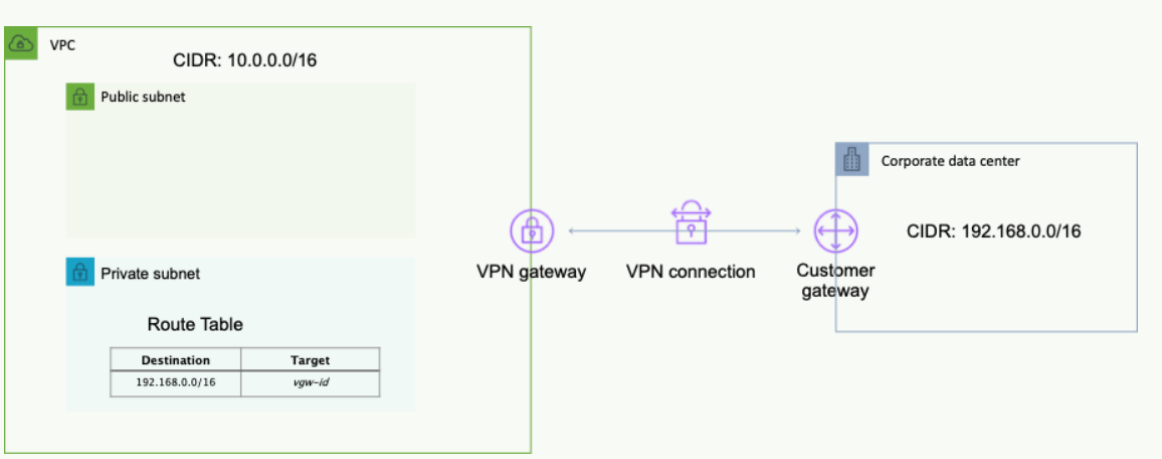
- Amazon DynamoDB может дросселировать запросы, которые превышают установленную пропускную способность для таблицы. **When requests will be throttled, and fail with an HTTP 400 code (Bad Request) and a ProvisionedThroughputExceededException**
  При использовании модели ценообразования с предоставлением емкости DynamoDB не масштабируется автоматически. DynamoDB может автоматически масштабироваться при использовании нового режима предоставления емкости по требованию, однако это не настроено для данной базы данных.
- A CloudWatch Events rule can be used to set up automatic email notifications for Medium to High Severity findings to the email address of your choice. You simply create an Amazon SNS topic and then associate it with an Amazon CloudWatch events rule.
- Используйте шлюз AWS Direct Connect для подключения ваших VPC. Вы связываете шлюз AWS Direct Connect с одним из следующих шлюзов:
  - Транзитный шлюз при наличии нескольких VPC в одном регионе.
  - Виртуальный частный шлюз



- AWS рекомендует использовать AWS SDK для выполнения программных вызовов API к IAM. Однако вы также можете использовать IAM Query API для прямых вызовов веб-службы IAM. Для аутентификации при использовании API Query необходимо использовать идентификатор ключа доступа и секретный ключ доступа.

- Крупные миграции данных с помощью AWS DMS могут включать многие терабайты информации. Этот процесс может быть громоздким из-за ограничений пропускной способности сети или просто огромного объема данных. AWS DMS может использовать Snowball Edge и Amazon S3 для миграции больших баз данных быстрее, чем при использовании других методов.
- Наиболее экономически эффективное решение для обеспечения резервного копирования соединения Direct Connect - это соединение Direct Connect, и IPSec VPN. Они активны и рекламируются с помощью протокола Border Gateway Protocol (BGP).
- **AWS Global Accelerator** использует статические IP-адреса в качестве фиксированных точек входа для вашего приложения. Вы можете перенести до двух диапазонов адресов /24 IPv4 и выбрать, какие IP-адреса /32 использовать при создании ускорителя.
  Это решение гарантирует, что компания сможет продолжать использовать те же IP-адреса, и она сможет направлять трафик на конечную точку приложения в регионе AWS, ближайшем к конечному пользователю. Трафик передается по глобальной сети AWS для обеспечения стабильной производительности.
- SSD, General Purpose (GP2) provides 3 IOPS per GB up to 16,000 IOPS. Volume size is 1 GB to 16 TB.
- The key requirement is to limit the number of requests per second that hit the application. This can only be done by implementing throttling rules on the API Gateway. Throttling enables you to throttle the number of requests to your API which in turn means less traffic will be forwarded to your application server.
- File gateway предоставляет виртуальный локальный файловый сервер, который позволяет хранить и извлекать файлы как объекты в Amazon S3. Он может использоваться для локальных приложений, а также для резидентных приложений Amazon EC2, которым требуется хранение файлов в S3 для объектных рабочих нагрузок. Используется только для плоских файлов, хранящихся непосредственно на S3. Файловый шлюз предлагает доступ к данным в Amazon S3 на основе SMB или NFS с локальным кэшированием.
- Агент контейнеров ECS включен в оптимизированный AMI Amazon ECS, а также может быть установлен на любом экземпляре EC2, поддерживающем спецификацию ECS (поддерживается только на экземплярах EC2). Поэтому вам не нужно проверять, установлен ли агент.

- Необходимо убедиться, что установленный агент запущен и что профиль экземпляра IAM имеет необходимые разрешения.
  Шаги по устранению неполадок для контейнеров включают:
  - Убедитесь, что демон Docker запущен на экземпляре контейнера.
  - Убедитесь, что демон Docker Container запущен на экземпляре контейнера.
  - Убедитесь, что агент контейнера запущен на экземпляре контейнера.
  - Убедитесь, что профиль экземпляра IAM имеет необходимые разрешения.
- Транзитное шифрование Amazon ElastiCache - это дополнительная функция, которая позволяет повысить безопасность ваших данных в наиболее уязвимых местах - когда они находятся в пути из одного места в другое. ElastiCache for Redis at-rest encryption is an optional feature to increase data security by encrypting on-disk data. This does not encrypt the data in-transit when it is being replicated between nodes.
- Чтобы ваша функция Lambda могла получить доступ к ресурсам внутри вашего частного VPC, вы должны предоставить дополнительную информацию о конфигурации, специфичную для VPC, которая включает идентификаторы подсети VPC и идентификаторы групп безопасности. AWS Lambda использует эту информацию для настройки эластичных сетевых интерфейсов (ENI), которые позволяют вашей функции работать.
- CloudFront dictribution - is a content delivery network (CDN) that caches content to improve performance
- AWS CloudFormation предоставляет два метода обновления стеков: прямое обновление или создание и выполнение наборов изменений. При прямом обновлении стека вы отправляете изменения, и AWS CloudFormation немедленно развертывает их.
  Используйте прямое обновление, когда вы хотите быстро развернуть свои обновления. С помощью наборов изменений вы можете предварительно просмотреть изменения, которые AWS CloudFormation внесет в ваш стек, а затем решить, применять ли эти изменения.
- Amazon FSx for Windows File Server предоставляет полностью управляемое, высоконадежное и масштабируемое файловое хранилище, доступное по стандартному протоколу Server Message Block (SMB). Это наиболее подходящее место назначения для данного сценария использования.

- AWS DataSync можно использовать для перемещения больших объемов данных в режиме онлайн между местным хранилищем и Amazon S3, Amazon EFS или Amazon FSx for Windows File Server. В качестве исходного хранилища данных могут выступать файловые серверы Server Message Block (SMB).
- Для узлов приложения HPC рекомендуется использовать либо расширенную сеть, либо адаптер Elastic Fabric Adapter (EFA). Это поможет снизить задержки. Кроме того, группа размещения кластеров объединяет экземпляры близко друг к другу в зоне доступности.
- Использование группы размещения кластеров позволяет рабочим нагрузкам достичь производительности сети с низкой задержкой, необходимой для тесно связанной связи между узлами, характерной для приложений HPC.
- 

CORRECT: “Configure a Virtual Private Gateway” is the correct answer.
- Amazon SNS supports notifications over multiple transport protocols:
  – HTTP/HTTPS – subscribers specify a URL as part of the subscription registration.
  – Email/Email-JSON – messages are sent to registered addresses as email (text-based or JSON-object).
  – SQS – users can specify an SQS standard queue as the endpoint.
  – SMS – messages are sent to registered phone numbers as SMS text messages.

Practice Set 5

-