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

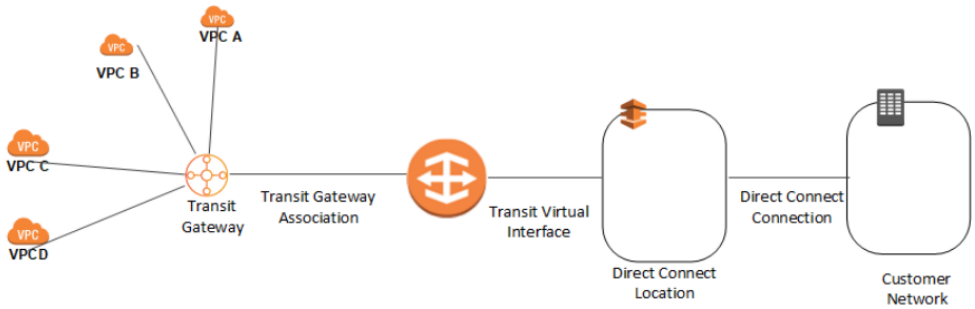
- Expedited — Expedited retrievals allow you to quickly access your data when occasional urgent requests for a subset of archives are required. For all but the largest archives (250 MB+), data accessed using Expedited retrievals are typically made available within 1–5 minutes. Provisioned Capacity ensures 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.

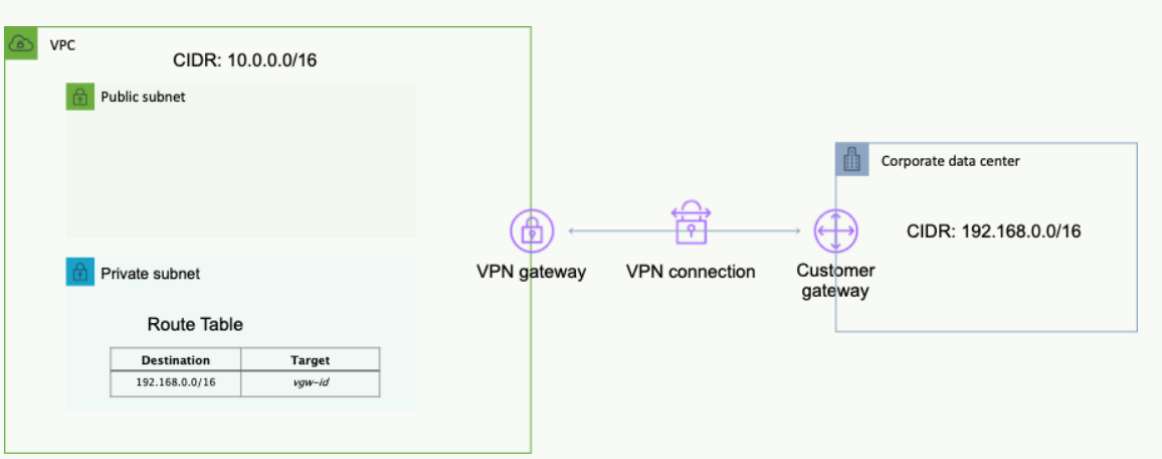
- Amazon DynamoDB может дросселировать запросы, которые превышают установленную пропускную способность для таблицы. **When requests will be throttled, and fail with an HTTP 400 code (Bad Request) and a ProvisionedThroughputExceededException**
  При использовании модели ценообразования с предоставлением 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

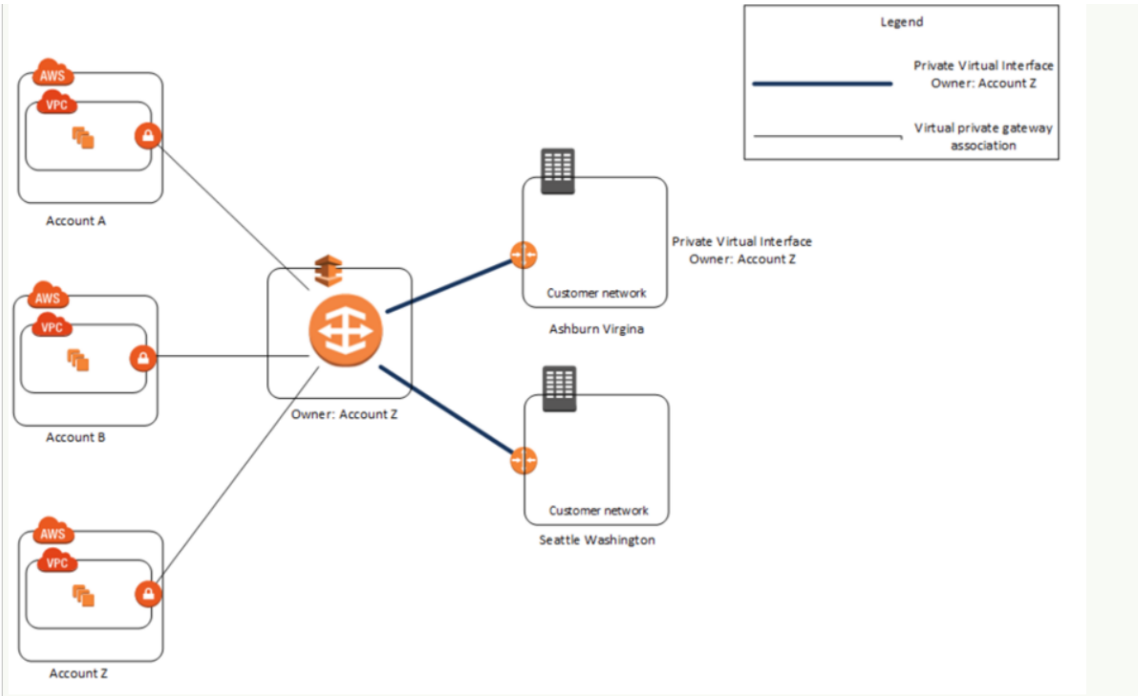
- Scheduled Instances are a good choice for workloads that do not run continuously but do run on a regular schedule. This is ideal for the development environment.

- Потоки данных Amazon Kinesis собирают и обрабатывают данные в режиме реального времени. Поток данных Kinesis представляет собой набор shard. Каждый shard содержит последовательность записей данных. Каждая запись данных имеет порядковый номер, который присваивается Kinesis Data Streams. Shard - это уникально идентифицированная последовательность записей данных в потоке.
  Partition key используется для группировки данных по разделам в потоке. Kinesis Data Streams разделяет записи данных, принадлежащие потоку, на несколько хранилищ. Он использует partition key, связанный с каждой записью данных, чтобы определить, к какому хранилищу принадлежит данная запись данных.
- Новая версия AWS Web Application Firewall была выпущена в ноябре 2019 года. В AWS WAF classic вы создаете "условия соответствия IP", тогда как в AWS WAF (новая версия) вы создаете "утверждения соответствия набора IP". Обратите внимание на формулировку на экзамене.
  Условие соответствия IP / утверждение соответствия набора IP проверяет IP-адрес происхождения веб-запроса на соответствие набору IP-адресов и диапазонов адресов. Используйте его для разрешения или блокирования веб-запросов на основе IP-адресов, с которых они исходят.
- **ALB поддерживает маршрутизацию как на основе путей** (например, /images или /orders), так и на основе хостов (например, example.com).
- AWS Lambda has a maximum execution time of 900 seconds (15 minutes).
- Архитектура уже обладает высокой устойчивостью, но при внезапном увеличении количества запросов может снизиться производительность. Для разрешения этой ситуации можно использовать Amazon Aurora Read Replicas для обслуживания трафика чтения, что разгрузит запросы от основной базы данных. На фронтенде перед ALB можно разместить дистрибутив Amazon CloudFront, который будет кэшировать содержимое для повышения производительности, а также разгрузит запросы с бэкенда.
- Существует два различных типа конечных точек VPC: конечная точка интерфейса и конечная точка шлюза. При использовании интерфейсной конечной точки вы используете ENI в VPC. При использовании конечной точки шлюза вы настраиваете таблицу маршрутов так, чтобы она указывала на конечную точку. Amazon S3 и DynamoDB используют конечные точки шлюза. Это решение означает, что весь трафик будет проходить через конечную точку VPC прямо к DynamoDB, используя частные IP-адреса.

- AWS Global Accelerator использует огромную, свободную от перегрузок глобальную сеть AWS для маршрутизации трафика TCP и UDP к здоровой конечной точке приложения в ближайшем к пользователю регионе AWS. Это означает, что он интеллектуально направляет трафик в ближайшую точку присутствия (уменьшая задержку). Бесперебойная обкатка гарантирована, так как AWS Global Accelerator использует anycast IP-адрес, что означает, что IP не меняется при обкатке между регионами, поэтому нет проблем с неправильными записями в клиентских кэшах, которые должны истечь.
- AWS Glue - это полностью управляемый сервис извлечения, преобразования и загрузки (ETL), который упрощает клиентам подготовку и загрузку данных для аналитики.
  С помощью этого решения уведомления о событиях S3, запускающие функцию Lambda, являются полностью бессерверными и экономически эффективными, а AWS Glue может запускать задания ETL, которые преобразуют эти данные и загружают их в хранилище данных, такое как S3.
- Amazon DynamoDB - это полностью управляемая служба баз данных NoSQL, которая обеспечивает быструю и предсказуемую производительность с плавным масштабированием. Кнопочное масштабирование означает, что вы можете масштабировать БД в любое время без простоя. DynamoDB обеспечивает низкую задержку при чтении и записи.
- Масштабирование по расписанию позволяет задать собственный график масштабирования для предсказуемых изменений нагрузки. Чтобы настроить группу Auto Scaling на масштабирование по расписанию, вы создаете запланированное действие. Это идеально подходит для ситуаций, когда вы знаете, когда и на какой срок вам понадобится дополнительная мощность.

- The cooldown period - это настраиваемый параметр для группы автоматического масштабирования, который помогает убедиться, что она не запускает и не завершает дополнительные экземпляры до того, как предыдущая активность масштабирования вступит в силу, так что это поможет. После того как группа Auto Scaling динамически масштабируется с помощью простой политики масштабирования, она ожидает завершения периода охлаждения, прежде чем возобновить действия по масштабированию.
  Период оценки тревог CloudWatch - это количество самых последних точек данных, которые необходимо оценить при определении состояния тревоги. Это поможет, так как вы можете увеличить количество точек данных, необходимых для подачи сигнала тревоги.
- An egress-only Internet gateway - это горизонтально масштабируемый, избыточный и высокодоступный компонент VPC, который позволяет исходящую связь по IPv6 от экземпляров в вашем VPC к Интернету и не позволяет Интернету инициировать соединение IPv6 с вашими экземплярами.
- Используйте Amazon CloudFront для обслуживания приложения и запрета доступа в заблокированные страны - is the EASIEST method!
- Kinesis Data Firehose is the easiest way to load streaming data into data stores and analytics tools.
- **EFS:**
  - **Storage class** – EFS One Zone or EFS Standard
  - **Performance mode** – General Purpose or Max I/O
  - **Throughput mode** – Bursting or Provisioned
- Глобальные таблицы Amazon DynamoDB представляют собой полностью управляемое решение для развертывания многорегиональной, многомастерной базы данных. Это единственное представленное решение, обеспечивающее активно-активную конфигурацию, в которой чтение и запись могут осуществляться в нескольких регионах с полной двунаправленной синхронизацией.
- Вы можете использовать функцию Lambda для обработки уведомлений Amazon Simple Notification Service. Amazon SNS поддерживает функции Lambda в качестве цели для сообщений, отправляемых в тему. Это решение отделяет приложение Amazon EC2 от Lambda и обеспечивает вызов функции Lambda.

Practice Set 6

- 

CORRECT: "Associate the Direct Connect gateway to a virtual private gateway in account A and B" is the correct answer.

- Access Logs могут быть включены на ALB и настроены на хранение данных в ведре S3. Amazon EMR - это веб-служба, которая позволяет предприятиям, исследователям, аналитикам данных и разработчикам легко и экономически эффективно обрабатывать огромные объемы данных. В EMR используется размещенная платформа Hadoop, работающая на Amazon EC2 и Amazon S3.
- Совет по сдаче экзамена:
  Для предотвращения чтения старых "несвежих" данных = используйте сильно последовательное чтение
  Объяснение:
  Когда вы запрашиваете сильно последовательное чтение, DynamoDB возвращает ответ с самыми актуальными данными, отражающими обновления от всех предыдущих операций записи, которые были успешными.
  Однако такая последовательность имеет некоторые недостатки:
  - - A strongly consistent read может быть недоступно при задержке или сбое в сети. В этом случае DynamoDB может выдать ошибку сервера (HTTP 500).

    - - A strongly consistent read может иметь более высокую задержку, чем окончательно последовательное чтение.
    - - A strongly consistent read не поддерживаются в глобальных вторичных индексах.
    - - A strongly consistent read используют большую пропускную способность, чем конечно-последовательные чтения.
- Exam Tip
  the most secure architecture is to put only the ELB in the public subnet and all other resources must be in a private subnet
- Configure AWS Organizations. Create an organizational unit (OU) and place all AWS accounts into the OU. Apply a service control policy (SCP) to the OU that denies the use of certain services.
- ELB connection draining can be used to stop sending requests to instances that are de-registering or unhealthy.
- Lambda может обрабатывать одновременные выполнения 1 000 в секунду на регион, и этот предел может быть увеличен.
- **Key Word "Scratch Data" = Use instance store.**
- the options "The time taken to run bootstrap scripts. & The size of embedded application code in the AMI" control warm up time for your instances.
- Чтобы ограничить доступ к содержимому, которое вы обслуживаете из ведер Amazon S3, выполните следующие действия:
    - 1. Создайте специального пользователя CloudFront, называемого идентификатором доступа к источнику (OAI), и свяжите его с вашим дистрибутивом.
    - 2. Настройте разрешения ведра S3 так, чтобы CloudFront мог использовать OAI для доступа к файлам в вашем ведре и предоставления их вашим пользователям. Убедитесь, что пользователи не могут использовать прямой URL-адрес к ведру S3 для доступа к файлу.
        - После выполнения этих действий пользователи смогут получить доступ к вашим файлам только через CloudFront, а не напрямую из ведра S3.
- Keyworkd "Web sockets" = Application load balancer.
  Application Load Balancers provide native support for WebSockets. You can use WebSockets with both HTTP and HTTPS listeners.

- Сценарий "fanout" - это когда сообщение Amazon SNS отправляется в тему, а затем реплицируется и отправляется в несколько очередей Amazon SQS, конечных точек HTTP или адресов электронной почты. Это позволяет выполнять параллельную асинхронную обработку. Например, можно разработать приложение, которое отправляет сообщение Amazon SNS в тему каждый раз, когда оформляется заказ на товар. Затем очереди Amazon SQS, подписанные на эту тему, будут получать идентичные уведомления о новом заказе. Серверный экземпляр Amazon EC2, подключенный к одной из очередей, может обрабатывать или выполнять заказ, а другой серверный экземпляр может быть подключен к хранилищу данных для анализа всех полученных заказов.
- No of GET/HEAD requests per second per prefix in a bucket is 5,500 .
  No of bucket prefixes = 5.
  total number of read request = 5500 * 5 = 27,500 read requests per second.
- С помощью S3 Object Lock вы можете хранить объекты по модели "запись-единственное-чтение-много" (WORM). С ее помощью можно предотвратить удаление или перезапись объекта на определенный период времени или на неопределенный срок. Блокировка объектов поможет вам выполнить нормативные требования, требующие хранения WORM, или просто добавить еще один уровень защиты от изменений и удаления объектов.
- Amazon EFS обеспечивает безопасный доступ для тысяч соединений для экземпляров Amazon EC2 и локальных серверов одновременно, используя традиционную модель разрешений файлов, возможности блокировки файлов и иерархическую структуру каталогов по протоколу NFSv4. Установки Amazon EC2 могут получить доступ к вашей файловой системе через AZ, регионы и VPC, а локальные серверы - через AWS Direct Connect или AWS VPN.
-

Practice Set 7

- Deployment approach:
  развернуть приложение на всех узлах одновременно = **использовать All-at-once**
  При развертывании на вычислительной платформе Amazon ECS в конфигурации развертывания указывается, как трафик переключается на обновленный набор задач Amazon ECS.
  - Существует три способа перераспределения трафика во время развертывания:
    - **Canary:** Трафик смещается в два этапа. Можно выбрать один из предопределенных вариантов Canary, который определяет процент трафика, переводимого на обновленный набор задач Amazon ECS в первом приращении, и интервал в минутах до перевода оставшегося трафика во втором приращении.
    - **Linear:** Трафик переключается равными порциями с равным количеством минут между каждой порцией. Вы можете выбрать из предопределенных линейных опций, которые определяют процент трафика, смещаемого в каждом приращении, и количество минут между каждым приращением.
    - **All-at-once:** Весь трафик перемещается с исходного набора задач Amazon ECS на обновленный набор задач Amazon ECS одновременно.
- **Amazon ECS с Fargate Launch Type** - используется, если вам нужно запускать контейнеры без необходимости управлять серверами или кластерами экземпляров Amazon EC2.
  AWS Fargate - это технология, которую вы можете использовать с Amazon ECS для запуска контейнеров без необходимости управления серверами или кластерами экземпляров Amazon EC2. С AWS Fargate вам больше не нужно предоставлять, настраивать или масштабировать кластеры виртуальных машин для запуска контейнеров. Это устраняет необходимость выбирать типы серверов, решать, когда масштабировать кластеры, или оптимизировать упаковку кластеров.
  При запуске задач и служб с типом запуска Fargate вы упаковываете приложение в контейнеры, указываете требования к процессору и памяти, определяете сетевые политики и политики IAM и запускаете приложение. Каждая задача Fargate имеет свою собственную границу изоляции и не разделяет базовое ядро, ресурсы ЦП, память или эластичный сетевой интерфейс с другой задачей.

- **Configure the TTL** - единственный способ управления кэшированием в Amazon API Gateway.
  Вы можете включить кэширование API в Amazon API Gateway, чтобы кэшировать ответы вашей конечной точки. С помощью кэширования можно сократить количество обращений к конечной точке, а также улучшить задержку запросов к API.
  Когда вы включаете кэширование для этапа, API Gateway кэширует ответы от вашей конечной точки в течение определенного 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.
- **С вас НЕ взимается плата за НЕПОЛНЫЙ ЧАС использования**, если цена Spot превышает вашу максимальную цену и Amazon EC2 прерывает работу вашего Spot Instance.
- To restrict users based on their location = Use Amazon CloudFront Geo Restriction.
- Use **Cross-Origin Resource Sharing (CORS)** to allow allow communication between applications from different domains.
- IPv6 traffic to the Internet = Use an egress-only internet gateway!
- Чтобы сопоставить домен с другим доменом, используйте запись CNAME.

- Благодаря поддержке SNI мы упрощаем использование более одного сертификата с одним и тем же ALB. Наиболее распространенная причина, по которой вам может понадобиться использовать несколько сертификатов, - это **работа разных доменов с одним и тем же балансировщиком нагрузки**. Всегда было возможно использовать сертификаты с подстановочными знаками и сертификаты с альтернативными именами субъектов (SAN) с ALB, но они имеют свои ограничения. Сертификаты Wildcard работают только для связанных поддоменов, которые соответствуют простому шаблону, а сертификаты SAN могут поддерживать множество различных доменов, но при этом один и тот же центр сертификации должен аутентифицировать каждый из них. Это означает, что вам придется заново проходить аутентификацию и заново предоставлять сертификат каждый раз, когда вы добавляете новый домен.

  Браузеры, поддерживающие SNI, во время инициализации защищенного соединения немедленно сообщают имя веб-сайта, к которому хочет подключиться посетитель, чтобы сервер знал, какой сертификат отправить обратно. Это позволяет браузерам/клиентам и серверам, поддерживающим SNI, подключать несколько сертификатов для нескольких доменов к одному IP-адресу. Таким образом, посетитель вашего сайта не заметит никаких различий.

  Балансировщик нагрузки использует интеллектуальный алгоритм выбора сертификата с поддержкой SNI. Если имя хоста, предоставленное клиентом, совпадает с одним сертификатом в списке сертификатов, балансировщик нагрузки выбирает этот сертификат. Если имя хоста, предоставленное клиентом, соответствует нескольким сертификатам в списке сертификатов, балансировщик нагрузки выбирает лучший сертификат, который может поддерживать клиент. Выбор сертификата основывается на следующих критериях в следующем порядке:
  - a - Алгоритм открытого ключа (предпочтительнее ECDSA, чем RSA)
  - b - Алгоритм хэширования (предпочтительнее SHA, чем MD5)
  - c - Длина ключа (предпочтительнее наибольшая)
  - d - Срок действия

- Действия, которые могут быть настроены в случае прекращения работы экземпляра **Spot**:
    1. hibernate
    2. stop
    3. terminate
- Для создания быстрого хранилища сессий для ваших онлайн-приложений = Используйте **Amazon ElastiCache** для Redis!
- Экономически эффективное и масштабируемое хранилище + хранение картографических данных в сотнях файлов данных + возможность роста до десятков терабайт = стандарт Amazon S3.
- To route a trafic to static pages hosted on Amazon S3 , you must have:
    - a – registered domain name.
    - b – The bucket must have the same name as your domain or subdomain
- **Вы можете использовать следующие механизмы для аутентификации и авторизации в API Gateway:**
    - Политики ресурсов позволяют создавать политики на основе ресурсов для разрешения или запрета доступа к API и методам с указанных IP-адресов источников или конечных точек VPC.
    - Стандартные роли и политики AWS IAM обеспечивают гибкий и надежный контроль доступа, который можно применять ко всему API или отдельным методам. Роли и политики IAM можно использовать для контроля над тем, кто может создавать и управлять вашими API, а также над тем, кто может их вызывать.
    - Теги IAM могут использоваться вместе с политиками IAM для контроля доступа.
    - Политики конечных точек для конечных точек интерфейса VPC позволяют прикреплять политики ресурсов IAM к конечным точкам интерфейса VPC для повышения безопасности ваших частных API.
    - Авторизаторы Lambda - это функции Lambda, которые контролируют доступ к методам REST API, используя аутентификацию по маркеру предъявителя, а также информацию, описанную в заголовках, путях, строках запроса, переменных этапа или параметрах запроса контекстных переменных. Авторизаторы Lambda используются для управления тем, кто может вызывать методы REST API.

    - Пулы пользователей Amazon Cognito позволяют создавать настраиваемые решения аутентификации и авторизации для ваших REST API. Пулы пользователей Amazon Cognito используются для управления тем, кто может вызывать методы REST API.

- Для подключения elastic network interface (ENI) к работающему экземпляру EC2 - необходимо использовать **Hot attach**!

  Вы можете присоединить сетевой интерфейс к экземпляру во время его работы (**Hot attach**), во время его остановки (**Warm attach**) или во время запуска экземпляра (**Cold attach**).
    - Можно отсоединить вторичные сетевые интерфейсы, когда экземпляр запущен или остановлен. Однако нельзя отсоединить первичный сетевой интерфейс.
    - Можно переместить сетевой интерфейс с одного экземпляра на другой, если экземпляры находятся в одной зоне доступности и VPC, но в разных подсетях.
    - При запуске экземпляра с помощью CLI, API или SDK можно указать основной сетевой интерфейс и дополнительные сетевые интерфейсы.
    - Запуск экземпляра Amazon Linux или Windows Server с несколькими сетевыми интерфейсами автоматически настраивает интерфейсы, частные адреса IPv4 и таблицы маршрутизации в операционной системе экземпляра.
    - При теплом или горячем подключении дополнительного сетевого интерфейса может потребоваться вручную вызвать второй интерфейс, настроить частный IPv4-адрес и соответствующим образом изменить таблицу маршрутизации. Экземпляры под управлением Amazon Linux или Windows Server автоматически распознают теплое или горячее подключение и настраиваются самостоятельно.
    - Присоединение еще одного сетевого интерфейса к экземпляру (например, конфигурация NIC teaming) не может использоваться как метод увеличения или удвоения пропускной способности сети к или от экземпляра с двойным подключением.

    - При подключении к экземпляру двух или более сетевых интерфейсов из одной подсети вы можете столкнуться с сетевыми проблемами, такими как асимметричная маршрутизация. Если возможно, используйте вторичный частный IPv4-адрес на основном сетевом интерфейсе.

- Если удаленный объект все еще существует в ведре Amazon S3, поскольку запросы Amazon S3 DELETE в конечном счете последовательны.
  Amazon S3 обеспечивает конечную согласованность для DELETES во всех регионах AWS. Кроме того, Amazon S3 реплицирует данные на нескольких серверах. Это означает, что когда вы удаляете объект, может потребоваться некоторое время для репликации удаления на всех серверах.

- В рабочих нагрузках машинного обучения используются огромные объемы обучающих данных. В этих рабочих нагрузках часто используется общее файловое хранилище, поскольку несколько вычислительных экземпляров должны обрабатывать обучающие данные одновременно. FSx для Lustre оптимален для рабочих нагрузок машинного обучения, поскольку он обеспечивает общее файловое хранилище с высокой пропускной способностью и постоянными низкими задержками для обработки учебных наборов данных ML. FSx for Lustre также интегрирован с Amazon SageMaker, что позволяет ускорить выполнение заданий на обучение.
- **Protecting the infrastructure is the main responsibility at Amazon Side.**
- By default, AWS has a limit of 20 instances per region. This includes all instances set up on your AWS account.
  To increase EC2 limits, request a higher limit by providing information about the new limit and regions where it should be applied.
- Each device has different storage capacities, as follows:

Storage capacity (usable capacity)	Snowball	Snowball Edge
50 TB (42 TB usable) - US regions only	✓	
80 TB (72 TB 72 usable)	✓	
100 TB (83 TB usable)		✓
100 TB Clustered (45 TB per node)		✓

- To access AWS Systems Manager APIs from your VPC without accessing the internet = Use AWS PrivateLink!
- Accessed and shared across multiple VPC + store up to 3300 keys+ integrated with AWS CloudTrail + support MFA = **AWS CloudHSM**
- To audit log of any changes made to AWS resources in their account = Use AWS CloudTrail.
- **Auto complete** is a good feature in Use ElastiCache with Redis.
- To reflect the **updates immediately** in **CloudFormation** - Use **Direct update**!
- Для предотвращения подслушивания при общении с ELB = использовать функцию Perfect Forward Secrecy.
  Perfect Forward Secrecy - это функция, которая обеспечивает дополнительную защиту от подслушивания зашифрованных данных благодаря использованию уникального случайного сеансового ключа. Это предотвращает расшифровку перехваченных данных, даже если секретный долгосрочный ключ скомпрометирован.
- To monitor API calls = Use custom CloudWatch matrix.

Practice Set 8

-
- Real-time notifications based using Amazon CloudWatch = CloudWatch **Events**
- Перенос системы обмена сообщениями в AWS + низкая стоимость = Amazon MQ
- to remove CloudFront caches before expiration =**Invalidate the files**.
- для поддержки ожидаемого роста = добавить больше реплик для чтения + переместить статические файлы из ECS в S3
- track session data + no downtime = Use DynamoDB
- to perform processing on a files in S3 bucket = Use S3 event + Amazon Lambda Function

- Чтобы ограничить доступ к содержимому, которое вы предоставляете из ведер Amazon S3, выполните следующие действия:
  - Создайте специального пользователя CloudFront, называемого идентификатором доступа к источнику (OAI), и свяжите его с вашим дистрибутивом.
  - Настройте разрешения ведра S3 так, чтобы CloudFront мог использовать OAI для доступа к файлам в вашем ведре и предоставления их вашим пользователям. Убедитесь, что пользователи не могут использовать прямой URL-адрес к ведру S3 для доступа к файлу.
- **At EC2 level we cannot use WAF because AWS WAF is used to control how an Amazon CloudFront distribution, an Amazon API Gateway API, or an Application Load Balancer responds to web requests.**
- для балансировки запросов по нескольким репликам чтения Aurora = Использовать конечную точку Aurora Reader
- Расширение локальных сетей в облако и безопасный доступ к ним из любого места = использование VPN
- Защита данных - это защита данных во время их транспортировки (когда они перемещаются в Amazon S3 и обратно) и в состоянии покоя (когда они хранятся на дисках в центрах обработки данных Amazon S3). Данные в пути можно защитить с помощью протокола Secure Sockets Layer (SSL) или шифрования на стороне клиента. У вас есть следующие варианты защиты данных в состоянии покоя в Amazon S3:
  - Шифрование на стороне сервера - запрос к Amazon S3 на шифрование объекта перед сохранением его на дисках в центрах обработки данных, а затем расшифровка при загрузке объектов.
  - Шифрование на стороне клиента - шифрование данных на стороне клиента и загрузка зашифрованных данных в Amazon S3. В этом случае вы управляете процессом шифрования, ключами шифрования и соответствующими инструментами.
- для ускорения загрузки изображений = Используйте Amazon CloudFront
- to provide High availability for Amazon ElastiCache for Redis = Configure ElastiCache Multi-AZ .

- Amazon RDS обнаруживает и автоматически восстанавливается после наиболее распространенных сценариев отказа в развертываниях Multi-AZ, чтобы вы могли как можно быстрее возобновить работу базы данных без вмешательства администратора. Amazon RDS автоматически выполняет обход отказа в случае любого из следующих событий:
  - Потеря доступности в основной зоне доступности
  - Потеря сетевого подключения к первичному серверу
  - Отказ вычислительного блока на первичном сервере
  - Отказ системы хранения данных на основной базе
- to simplify AWS infrastructure with providing IP multicast = Use AWS Transit Gateway
- Amazon DynamoDB интегрирована с AWS Lambda, поэтому вы можете создавать триггеры - части кода, которые автоматически реагируют на события в потоках DynamoDB. С помощью триггеров можно создавать приложения, реагирующие на изменения данных в таблицах DynamoDB. Если вы включите потоки DynamoDB для таблицы, вы можете связать потоковое имя ресурса Amazon (ARN) с написанной вами функцией AWS Lambda. Сразу же после изменения элемента в таблице в потоке таблицы появляется новая запись. AWS Lambda опрашивает поток и вызывает вашу функцию Lambda синхронно, когда обнаруживает новые записи в потоке.
- AWS Security Token Service (AWS STS) - это веб-служба, которая позволяет запрашивать временные учетные данные с ограниченными привилегиями для пользователей AWS Identity and Access Management (IAM) или для пользователей, которых вы аутентифицируете (объединенные пользователи). В данном руководстве описывается API AWS STS.
- No of PUT requests per second per prefix in a bucket is 3,500 .
  - No of bucket prefixes = 3
  - total number of read request = 3500 * 3 = 10,500 PUT requests per second
  - For example, your application can achieve at least 3,500 PUT/COPY/POST/DELETE or 5,500 GET/HEAD requests per second per prefix in a bucket.
-

Practice Set 9

- Strong consistency = DynamoDB
- Handle failed messages = Amazon SQS dead-letter queue.
  Amazon SQS поддерживает очереди с мертвыми буквами, которые другие очереди (очереди-источники) могут использовать для сообщений, которые не могут быть успешно обработаны (потреблены). Очереди с мертвыми буквами полезны для отладки приложения или системы обмена сообщениями, поскольку они позволяют изолировать проблемные сообщения, чтобы определить, почему их обработка не удалась.
- RDS Storage Auto Scaling постоянно отслеживает фактическое потребление хранилища и автоматически масштабирует емкость, когда фактическое использование приближается к предоставленному объему хранилища. Автомасштабирование работает с новыми и существующими экземплярами баз данных. Вы можете включить функцию автоматического масштабирования всего несколькими щелчками мыши в консоли управления AWS. Автомасштабирование хранилища RDS не требует дополнительных затрат. Вы платите только за ресурсы RDS, необходимые для работы ваших приложений.
- To protect the application from DDOS attach = **Use AWS Shield**
- Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer
- Can concurrently run **20000 requests** or functions + Scalable = using **docker container** on Amazon ECS.
  But **Lambda has a limitation of 1000 concurrent requests**
  Your functions' concurrency is the number of instances that serve requests at a given time. For an initial burst of traffic, your functions' cumulative concurrency in a Region can reach an initial level of between 500 and 3000, which varies per Region.
  Burst concurrency limits for Lambda:
  - 3000 – US West (Oregon), US East (N. Virginia), Europe (Ireland)
  - 1000 – Asia Pacific (Tokyo), Europe (Frankfurt)
  - 500 – Other Regions
- Simplify inventory and compliance management across accounts and regions = **AWS Config**
- S3, DynamoDB и Lambda имеют HA, только PostgreSQL пока не имеет... Просто включите его.
- Пояснение

- PostgreSQL стал предпочтительной реляционной базой данных с открытым исходным кодом для многих корпоративных разработчиков и стартапов, обеспечивая работу ведущих бизнес- и мобильных приложений. Amazon RDS упрощает настройку, эксплуатацию и масштабирование развертывания PostgreSQL в облаке. С помощью Amazon RDS вы можете развернуть масштабируемые системы PostgreSQL за считанные минуты, используя экономически эффективные и изменяемые аппаратные мощности. Amazon RDS решает сложные и трудоемкие административные задачи, такие как установка и обновление программного обеспечения PostgreSQL, управление хранилищем, репликация для обеспечения высокой доступности и пропускной способности чтения, а также резервное копирование для аварийного восстановления.
- **Enable** Amazon **DynamoDB Auto Scaling** = LESS changes
- A company has on-premises Microsoft Active Directory and wants to allow its employees to access it's multiple accounts in AWS using their user names and passwords - USE **AWS Single Sign On**
- **for HA , we need two Availability zone and each AZ contains 3 subnets (1 public for ALB + 1 private for Web servers + 1 private for Database).**
- AWS compute solution + **no special hardware** + use 512 MB of memory to run = AWS **Lambda functions**
- Amazon EC2 instance should stop rather than terminate when its Spot Instance is interrupted:
    - For a Spot Instance request, the type must be **persistent**. You cannot specify a launch group in the Spot Instance request.
    - For an EC2 Fleet or Spot Fleet request, the type must be **maintain**.
    - The root volume must be an **EBS volume**, not an instance store volume.

- **Выделенные хосты** Amazon EC2 позволяют использовать лицензии на программное обеспечение от таких производителей, как Microsoft и Oracle, на Amazon EC2, что обеспечивает гибкость и экономическую эффективность использования собственных лицензий, а также гибкость, простоту и эластичность AWS.
  Выделенный хост Amazon EC2 - это физический сервер, полностью выделенный для вашего использования, что поможет вам соответствовать корпоративным требованиям.

  Выделенные хосты позволяют использовать существующие лицензии на программное обеспечение на сокет, ядро или виртуальную машину, включая Windows Server, SQL Server, SUSE Linux Enterprise Server, Red Hat Enterprise Linux или другие лицензии на программное обеспечение, привязанные к виртуальным машинам, сокетам или физическим ядрам, в соответствии с условиями лицензии. Это поможет вам сэкономить деньги за счет использования существующих инвестиций. Узнайте больше о вариантах лицензирования Windows.
-