Добрый день, уважаемые студенты! Я рад вас всех видеть на очередной сессии Демо. Тема сегодняшней сессии – это часто встречающиеся сценарии на реальном экзамене AWS. Мы рассмотрим все популярные и возможные ответы в случае такого сценария. Итак, давайте начнем.

Перед тем, как мы начнем, я бы хотел указать источник, откуда эта информация была взята. Все вы, возможно, слышали, возможно, нет, но есть такой человек Джон Бонсо, достаточно яркая личность в сфере подготовки к экзаменам AWS. Все начиналось с того, что этот человек владел сайтом, на который закидывал гайды по определенным сервисам, т.е. берется какой-то сервис AWS Lambda и подготавливается для него тезисная информация об этом сервисе. И эта информация, она часто встречается на экзамене и довольно хорошо помогает повторить большую часть материала, читая эти тезисы. Они достаточно короткие и сжатые, и так было приготовлено для большей части сервисов. Далее, проект развивался буквально на глазах, и в какой-то момент появились тесты для подготовки к экзаменам AWS, опубликованные в Udemy. После чего этот проект вырос уже из Udemy и tutorialsdojo.com превратился в некий учебный портал, в котором начали появляться тесты. Есть движок тестирования, который подбирает вопросы, интерфейс улучшился. Через какое-то время наступил следующий шаг, подготовили дополнительный материал и уже появились не только разборы тестовых вопросов, но и целые курсы для подготовки к определенному экзамену AWS. Наряду со всем этим материалом также есть страницы, специально предназначенные для каждого экзамена AWS, которые рассматривают ее с разных сторон. И один кейс, это Common Exam Scenarios, как раз таки по этой ссылке вы можете напрямую перейти, либо в Google написать bonso aws cp, т.е. Cloud Practitioner и common scenarios, вы попадете на нужную вам страницу. Я достаточно позитивно высказался касательно ресурса, это действительно так, но есть один небольшой нюанс, который достаточно важен. Материала много, материал полезный. Из минусов это то, что он полностью на английском, это – первое. И второе – это то, что не все материалы, не вся информация, она актуальная. Поэтому какие-то цифры, точные факты рекомендуется перепроверять по документации AWS. Основные же концепции в целом редко меняются, и можно сказать, что вот такого рода информацию можно читать и воспринимать как актуальную на вот подобных сайтах. Возвращаемся обратно к нашим слайдам. Слайды организованы следующим образом: все слайды поделены на четыре направления, это старые домены экзамена AWS Certified Cloud Practitioner, сейчас пять доменов, но это никак не понижает ценность этой информации, а лишь помогает нам сгруппировать все кейсы по четырем различным направлениям. Сами слайды организованы следующим образом. Есть сценарии, там какое-то предложение либо часть предложения, описывающее наш сценарий и соответственно решение. Решением в большинстве случаев является один или несколько сервисов AWS, в каких-то случаях это определенный функционал внутри определенного сервиса, либо какое-то понятие и термин. Я бы здесь хотел особо отметить, что это не является шпаргалкой. Это больше материал для повторения студентам, которые прошли весь теоретический материал, и здесь как раз таки рассматриваются самые популярные кейсы, основные моменты, на которые стоит акцентировать, обратить внимание и дополнительно повторить. Поэтому для тех, кто только зашел на курс и сразу перешел на последнее Демо, это бесполезный материал, набор непонятных терминов. Для тех, кто планомерно двигался, это достаточно ценный материал, который вам поможет структурировать ваши знания. Более того, эти частые кейсы не только те кейсы, которые встречаются на экзамене AWS. Сам экзамен построен на том, чтобы помогать вам в будущем, когда вы будете работать с AWS. Поэтому внутри экзамена вопросы взяты из реальной жизни облачного инженера. И те кейсы, которые мы здесь разберем, вы также будете использовать, когда вы будете работать облачным инженером в одной из компаний. Хорошо, давайте начинаем, двигаемся дальше.

Первый домен, первая группа сценариев – это Cloud Concepts, т.е. основные понятия облачных технологий.

Итак, сценарий: Какие финансовые преимущества получает компания при миграции всех своих систем из локального дата-центра в AWS? Ответ: Первым ответом является то, что компания заменяет капитальные расходы на операционные расходы. Что это означает? Мы с вами говорили, что капитальные расходы это когда мы несем расходы наперед. Одним из ярких примеров – это покупка целого сервера, т.е. вы покупаете за большую сумму и вне зависимости от того вы будете использовать пять лет либо три месяца, вы должны оплатить всю сумму. Когда мы говорим операционные расходы, и в частности облако AWS, мы можем поднять достаточно мощный EC2 инстанс, использовать его три часа, оплатить только за три часа и после этого высвободить наши ресурсы для того чтобы не платить. Таким образом, мы можем все или большую часть капитальных расходов, когда мы владеем собственным дата-центром, перенести на операционные расходы и оплачивать только за то, что мы используем при переходе на AWS. Второй кейс – это reduce the total cost of ownership, т.е. идея такая же, когда мы владеем собственным локальным дата-центром, то в этом случае нам необходимо все закупать сразу. Возможно, у вас очень большие затраты пойдут на покупку помещения, либо ежемесячная трата на аренду. Далее у вас есть штат сотрудников, которые поддерживают работу дата-центра. Это те расходы, которые постоянные, не меняются. Даже если у вас на вашем сайте не будет ни одного пользователя, то вы все равно будете нести эти расходы. Когда же мы говорим про AWS, мы можем построить инфраструктуру таким образом, что она автомасштабируется и в большую и в меньшую сторону. И в случае, когда мы видим спад трафика, нет ни одного пользователя на нашем сайте, нет нагрузки, в этом случае инфраструктура может автоматически уменьшиться до минимальных размеров. Таким образом, мы будем нести также минимальные расходы на нашу инфраструктуру.

Сценарий: Укажите принципы построения архитектуры в облаке AWS. Ответы, решения: Первое – это Design for Failure. Идея в том, что при увеличении размеров вашей инфраструктуры пропорционально также увеличивается вероятность того, что где-то что-то пойдет не так, какой-то из компонентов сломается. Поэтому необходимо думать наперед, зная какие компоненты могут сломаться, добавлять либо избыточность, либо возможность быстрого авто-восстановления. Второе – Decouple your components. Идея в том, что нужно строить архитектуру таким образом, чтобы все компоненты были слабо связаны между собой. Зачем это нужно? При слабой связанности можно легко заменить каждый компонент. Более того, при поломке какого-то компонента оно меньше влияет на соседние компоненты. Таким образом, разрушительное влияние какой-то поломки будет уменьшено за счет вот такой архитектуры. Третье, четвертое – это связано Implement Elasticity, т.е. говорим про гибкость и Think Parallel – это про масштабирование. Идея в том, что у нас есть связка сервисов, при правильной настройке архитектура превращается в живой организм. И может в зависимости от некоторых метрик, например, нагрузки на ваши сервера, увеличиваться автоматически в размерах, как в большую, так и в меньшую сторону. Более подробно вы можете посмотреть наши принципы построения архитектур на лекционном занятии.

Сценарий: У нас есть критические нагрузки в облаке AWS, которые должны быть высоко доступны. Что необходимо использовать, как частое решение – это строить инфраструктуру на нескольких availability зонах. Таким образом, крайне вероятное событие выхода из строя целой одной availability зоны будет учтена и в случае, даже если произойдет это событие, ваша инфраструктура продолжит работать, но уже на оставшихся двух либо второй availability зоне.

Сценарий: Нам необходимо, чтобы изменение либо поломка одного из компонентов не эскалировало на другие компоненты, т.е. не переходило и не влияло, не ломало следующие компоненты, которые по соседству. Как решение строить архитектуру слабосвязную, т.е. loose coupling. Если мы говорим сильносвязные, т.е. соответствующий термин tight coupling. И нам необходимо стремиться строить архитектуру от tight coupling в сторону loose coupling.

Сценарий: У вас есть VPC, в VPC есть public subnet и внутри EC2 инстанс. Необходимо, чтобы этот EC2 инстанс мог выходить в общий интернет. Как решение, нам необходим Internet Gateway.

Сценарий: У вас есть настроенный VPC, внутри VPC есть private subnet и внутри private subnet EC2 инстанс. Необходимо, чтобы этот EC2 инстанс мог выходить в интернет. Так как в вопросе явно указано, что EC2 инстанс находится внутри private subnet, то ресурс, который дает доступ в интернет инстансам – это NAT Gateway. NAT Gateway настраивается в public subnet и мы настраиваем дополнительный route, чтобы направлять трафик из private subnet в NAT gateway в public subnet. Там далее уже на уровне VPC настраивается Internet Gateway, через который и выходит в интернет все ресурсы внутри вашего VPC.

Мы с вами переходим к следующему блоку сценариев – это security и compliance.

Сценарий: Укажите инструмент для настройки безопасности, а именно настройки WAF рулов поверх нескольких аккаунтов. Как ответ – это сервис AWS Firewall Manager.

Сценарий: Компании необходимо загрузить документы, подтверждающие соответствия AWS определенным регуляторным требованиям, либо требованиям стандартов. Ответ: Вам необходимо обратиться в сервис AWS Artifact, где загружены все эти документы, и вы можете по требованию эти документы скачать.

Сценарий: Что необходимо сделать для того, чтобы улучшить безопасность IAM пользователей? Первый ответ – это настроить Multi-Factor Authentication (MFA). Второй – это настроить достаточно сложное правило для пароли ваших пользователей.

Сценарий: Какая сущность IAM использует ассess ключи для доступа к ресурсам в облаке AWS через AWS CLI? Ответ: IAM User.

Сценарий: К какой сущности IAM мы предоставляем временный доступ к нашим AWS ресурсам. Ответ: IAM Role.

Сценарий: Что необходимо использовать для того, чтобы управлять доступами для большого количества IAM пользователей. Ответ: IAM Group.

Сценарий: Что мы можем использовать для того, чтобы предоставить доступ к нашим ресурсам в бакете Amazon S3? Ответ: Мы можем настроить Bucket policy, который привязан к бакету. Там вы указываете операции и пользователей, которые могут обращаться к вашему бакету. Можно настроить с другой стороны, а именно User Policy. Вы для каждого пользователя, для группы, либо для роли прописываете дополнительные policy о том, что эта policy дает доступ к определенным операциям, к таким-то ресурсам. Как ресурс мы указываем наши S3 бакеты.

Сценарий: Нам необходимо предоставить доступ к AWS через предоставление временных credential для пользователей. И эти пользователи, они авторизованы через социальные медиа, либо совсем могут быть не авторизованы, т.е. анонимные гости. Что мы можем использовать для того, чтобы это обеспечить? Как ответ использовать Amazon Cognito Identity Pool.

Сценарий: Вы являетесь стартапом и вам необходимо оценить, как работают ваши IAM policy. Для этого необходимо использовать IAM policy simulator.

Следующий сценарий: Необходимо указать сервис, который находит, классифицирует и защищает важную информацию, которая относится к PII, т.е. это информация, которая может идентифицировать личность, либо относится к интеллектуальной собственности. В этом случае необходимо воспользоваться сервисом Amazon Macie.

Сценарий: Укажите сервис, который мониторит весь ваш AWS аккаунт, для поиска различных угроз и подозрительной активности. Это сервис Amazon GuardDuty.

Сценарий: Вам необходимо запретить не авторизованное удаление объектов внутри S3 бакетов. Для этого необходимо настроить MFA и при удалении объектов доступ будет разрешен только тем сущностям, т.е. ролям, пользователям, у которых была пройдена MFA проверка.

Сценарий: Компании необходимо контролировать трафик между VPC subnets. Это относится как к входящему, так и исходящему трафику. Необходимо для этого использовать Network Access Control List (NACL).

Сценарий: Укажите, что является неким virtual firewall и работает для контроля трафика на уровне EC2 инстанса. Ответ: это Security Group.

Сценарий: Укажите сервис, который проводит автоматические проверки безопасности для ваших приложений. Это Amazon Inspector.

Мы с вами добрались до следующего блока сценариев, связанных с технологиями.

Сценарий: Компании необходимо начать использовать глобальную инфраструктуру AWS для того, чтобы улучшить доступность своих приложений, при этом чтобы они были доступны по любому статическому IP-адресу. В этом случае нам необходимо использовать AWS Global Accelerator.

Следующий сценарий: Нам необходимо безопасно передать в AWS сотни петабайтов данных. Что для этого можно использовать? Вы видите, что петабайт передавать по сети – это достаточно большой объем информации, это много времени, а много времени, соответственно, компания не всегда может ждать. Поэтому есть решение, когда AWS выгружает кейс, в котором у нас есть жесткие диски, вычислительная мощность и отправляет этот чемоданчик к нам в офис. Как только он приезжает, мы подключаем его к сети и можем в него загрузить большой объем информации по локальной сети, что намного быстрее. И после того, как мы закончили, мы этот чемоданчик возвращаем обратно и как только онадоходит до любого дата-центра AWS, они подключают уже к своей локальной сети и быстренько загружают его с локальной, с быстрой скоростью в инфраструктуру AWS. Есть несколько видов решений Snowball. Есть Snowball Edge, Snowball обычный, которые поменьше и есть Snowmobile, когда вам отправляет целый прицеп с машиной, и он добирается до вас и можно не только сотни петабайтов, а еще больше данных загрузить в этот мобильный дата-центр.

Сценарий: Укажите тип инстанса EC2, который позволяет вам перенести лицензии, привязанные к определенному хосту. Этот тип Dedicated Host.

Следующий сценарий: Укажите сервис, который мониторит всю активность внутри AWS и фиксирует все вызовы AWS API, будь оно через AWS Management Console, либо через AWS SDK. Этим сервисом является AWS CloudTrail. CloudTrail – это аналог черного ящика в самолете.

Сценарий: Укажите DNS веб-сервис внутри AWS, который является достаточно высокодоступным и масштабируемым. Этот сервис Amazon Route 53.

Следующий сценарий: Нам необходимо сохранять результаты сложных SQL-запросов для того, чтобы ускорить производительность наших приложений. Для этого нам необходимо использовать кэш-сервис – это Amazon ElastiCache.

Сценарий: Нам необходимо указать связку AWS сервисов, которые позволяют обслуживать статические файлы с наименьшей задержкой. Это – Amazon S3 и Amazon CloudFront.

Следующие сценарии: Необходимо указать сервис, который предоставляет автоматическое масштабирование вычислительных мощностей в зависимости от входящего трафика, для того чтобы улучшить доступность ваших приложений и сократить падение ввиду перегрузки ваших вычислительных мощностей. Ответом является AWS Auto Scaling.

Сценарий: Нам необходимо перенести базу данных MySQL с локального дата-центра на сервис Amazon RDS. Каким сервисом мы можем для этого воспользоваться? Есть отдельный сервис для миграции баз данных, называется AWS DMS, либо в развернутом виде AWS Database Migration Service.

Следующий сценарий: Нам необходимо настроить автоматический перенос на следующий класс хранения нечасто запрашиваемых данных внутри S3 бакета, для того чтобы сэкономить на хранении. Для этого нам необходимо воспользоваться S3 Lifecycle Policy.

Сценарий: Вам необходимо загрузить один большой объект в S3 несколькими частями для того, чтобы ускорить ее перенос. Что необходимо для этого сделать? Мы для этого можем воспользоваться функционалом сервиса S3 Multipart Upload. Идея ее в том, что наш файл делится на несколько маленьких частей и эти части отправляются по отдельности. В случае, если какая-то часть падает, ее можно отдельно отправить. Более того, вы можете отправлять все ваши файлы параллельно. Таким образом, в несколько раз ускоряется передача ваших файлов в облако AWS.

Следующий кейс: Необходимо для компании предоставить выделенный connection между локальным дата-центром и AWS VPC. Для этого нам необходимо воспользоваться сервисом AWS Direct Connect.

Сценарий: Укажите сервис машинного обучения, который позволяет нам анализировать медиа-файлы и извлекать полезную информацию. Здесь имеется в виду как медиа-файлы, это картинки и видеоматериалы и то, что мы можем извлечь, это тексты, различные кастомные предметы. Ответ – Amazon Rekognition.

Следующий сценарий: Необходимо указать сервис, который позволяет делать трассировку запросов пользователей внутри вашего приложения. Этот сервис AWS X-Ray, он часто используется в связке с AWS Lambda. Идея в том, что когда приходит запрос от ваших пользователей, неважно на ваш API, либо на ваш сайт, вы можете добавить к этому запросу некоторые уникальные значения. С этим уникальным значением этот запрос будет передаваться внутрь всей вашей инфраструктуры и обрабатываться. Таким образом, отслеживая этот уникальный ID, вы можете видеть, как и куда проходят ваши запросы, визуально оценить, где какие задержки и попробовать улучшить ваше приложение.

Следующий кейс: Компании необходимо получить информацию об Instance ID, публичных ключах, публичном IP адресе вашего EC2 инстанса, где эту информацию можно получить? Эту информацию можно получить в AWS Management Console, если открыть ваш EC2 инстанс, внизу откроется набор вкладок и выбрать вкладку Instance metadata. Там вся эта информация доступна.

Сценарий: Нам необходимо ускорить доставку нашего контента наших статических файлов по всему миру. Ответ – это воспользоваться сервисом Amazon CloudFront.

Следующий сценарий: Сервис, который позволяет нам создавать и деплоить инфраструктуру как код. Ответ очевиден – это AWS CloudFormation.

Сценарий: Нам необходимо настроить шифрование наших логов в AWS CloudTrail. Для этого необходимо воспользоваться специальным сервисом AWS Key Management Service. Чаще вы его будете встречать как AWS KMS.

Следующий сценарий: Необходимо выбрать сервис, который предоставляет базы данных для работы с JSON документами, т.е. это NoSQL базы данных, не структурированные данные. Ответ – Amazon DynamoDB.

На этом мы добрались к следующему блоку и поговорим про сценарии, связанные с Billing и Pricing.

Сценарий: Нам необходимо выбрать опцию, где подразумевается выделенный человек от AWS, который дополнительно помогает нам сопровождать нашу инфраструктуру в облаке. Ответ – это ТАМ, либо развернутый вариант Technical Account Manager.

Следующий сценарий: Нам необходимо выбрать инструмент, который периодически проверяет наш AWS Account, и дает рекомендации, чтобы следовать Best Practice AWS. Это – сервис AWS Trusted Advisor.

Следующий сценарий: Мы являемся стартапом, и нам необходимо рассчитать стоимость переноса наших приложений с локального дата-центра на AWS. Для этого мы можем воспользоваться отдельным приложением, инструментом, который называется AWS Total Cost of Ownership.

Следующий сценарий: Нам необходимо выбрать тип Reserved Instances, который позволяют менять семейство инстанса, тип инстанса и другие свойства наших EC2 инстансов. Правильный ответ – Convertible RI.

Сценарий: Нам необходимо выбрать тип EC2 инстансов, который позволяет получить скидку до 90%. Это – Spot instance. Здесь многие допускают ошибку и выбирают вариант либо Savings Plans либо Reserved Instances. И тот и другой вариант они предлагают скидку от 60 до 70%. В случае с Spot instance мы можем получить до 90% скидки, и это самый дешевый вариант EC2 инстансoв. Есть определенные нюансы, про которые мы говорили на наших лекциях.

Сценарий: Нам необходимо выбрать приложение, которое позволяет нам управлять всеми нашими policy из одного места, а также получать совокупный счет за услуги AWS по всем нашим AWS аккаунтам. Правильный ответ – это сервис AWS Organizations.

Следующий сценарий: Нам необходимо выбрать самый дешевый вариант хранения внутри S3, а именно мы говорим про копии баз данных, которые могут быть запрошены изредка и при этом мы можем подождать несколько минут. Идеальным вариантом для этого кейса является Amazon Glacier.

Сценарий: Необходимо выбрать сервис, который предоставляет нам прогнозные будущие расходы на базе наших текущих данных, на базе текущего использования сервисов AWS. Ответом является сервис AWS Cost Explorer.

Следующий сценарий: Нам необходимо категоризировать и отслеживать наши расходы на AWS на более подробном уровне. Для этого нам необходимо воспользоваться функционалом, который называется Cost Allocation Tags. Идея ее в том, что мы можем тегировать все наши ресурсы AWS в специально отведенном месте. Мы указываем, какие теги являются Cost Allocation Tag, после чего мы можем группировать и видеть наши расходы по выбранным нами тегам в сервисе AWS Cost Explorer, а также в любых других сервисах, которые работают с расходами на облако.

Сценарий: Что необходимо сделать компании, если нам нужно запустить VPC, который не входит в сервисные лимиты по умолчанию? Ответ: Необходимо создать ticket в техподдержку и запросить увеличение этого лимита, если оно является Soft limits.

Следующий сценарий: Нам необходимо выбрать самый выгодный вариант покупки Reserved Instances на один год. Ответом является All Upfront Reserved Instances. Как мы с вами помним, мы можем выбрать три варианта оплаты, когда No Upfront мы не вносим никакую оплату, лишь подписываем договор и ежемесячно продолжаем платить за использование наших ресурсов со скидкой. Следующий вариант – это Partial Upfront, какая-то часть со скидкой оплачивается сразу за один год либо за три года, в зависимости от того, какой договор подписываем. И оставшаяся часть она оплачивается дальше ежемесячно также со скидкой. И третий вариант, который дает наибольшее количество скидок – это All Upfront, когда делается расчет на выбранный период, рассчитывается скидка и та оставшаяся сумма к оплате должна быть переведена сразу, после чего ежемесячной оплаты за выбранные нами Reserved Instances уже не будет.

Сценарий: Вам необходимо объединить использование определенного ресурса, для того чтобы добраться до скидок по объемам. Для того чтобы получить эти скидки и объединить ваше использование, необходимо использовать Consolidated Billing. Его мы можем включить в сервисы AWS Organizations.

Следующий сценарий: Представим, что вы подготовили собственный кастомный AMI, и хотите ее продавать внутри AWS для других клиентов AWS. Для этого вы можете воспользоваться сервисом AWS Marketplace. Это место, где вы можете продавать различные кастомные ресурсы для других клиентов, в том числе ваши кастомные AMI.

На этом мы подошли к концу нашей Демо сессии. Я очень надеюсь, что вы узнали что-то новое сегодня. Еще раз напоминаю, что все то, что мы разобрали, все сценарии не являются стопроцентным ответом на вопросы из реального экзамена AWS, а лишь удобным форматом для повторения всего того материала, который вы прошли, для перепроверки себя. Помните, что каждый вопрос, который придет на экзамене AWS, должен быть вами индивидуально рассмотрен. Не всегда бывает, что тот ответ, который указан здесь, он является правильным ответом, потому как формулировка вопросов может меняться. Мы с вами помним, что достаточно большое количество новых вопросов добавляется в каждый экзамен AWS, и они не идут в зачёт. Таким образом, у AWS есть возможность очень часто в больших объемах добавлять новые вопросы, и могут появиться вопросы с небольшим подвохом. В целом, идея этих сценариев была в том, чтобы закрепить основные моменты, сделать акценты на популярных сценариях для того, чтобы не только помочь вам при сдаче экзамена AWS, но и дать вам те знания, освежить те моменты, которые пригодятся вам во время работы облачным инженером. Спасибо за внимание. Увидимся с вами на следующих наших активностях!