WEBVTT

00:00:00.000 --> 00:00:07.400

Добрый день, уважаемые студенты. Мы с вами начинаем разбор вопроса Practice Test-а.

00:00:07.400 --> 00:00:12.200

Согласно вопросу, компания обслуживает клиентов по всему миру.

00:00:12.200 --> 00:00:20.680

Эти клиенты обращаются к данным компании, хранящиеся на нескольких S3 bucket-ах.

00:00:20.680 --> 00:00:42.320

У каждого S3 bucket-а настроен CloudFront web distribution и на текущий момент необходимо доставлять контент для специфичного клиента, чтобы только этот клиент мог добираться до данных компаний.

00:00:42.320 --> 00:00:53.680

На текущий момент все клиенты могут обращаться к данным через S3 URL, а также через CloudFront distribution.

00:00:53.680 --> 00:01:01.480

Два различных отдельных URL ссылки, по которым они могут обращаться и загружать данные.

00:01:01.480 --> 00:01:07.000

Вам необходимо как Solutions Architect настроить следующую архитектуру.

00:01:07.000 --> 00:01:19.320

Приватные данные должны передаваться только через CloudFront, так чтобы защитить распространение ваших файлов.

00:01:19.320 --> 00:01:30.880

С учетом этих ограничений, вам нужно из предложенных вариантов выбрать два варианта, которые помогают это все имплементировать.

00:01:30.880 --> 00:01:36.720

На этом слайде вы видите варианты ответов, также видите, что второй и третий являются верными.

00:01:36.720 --> 00:01:41.320

Давайте посмотрим на объяснение.

00:01:41.320 --> 00:01:51.440

Вы видите на картинке, что есть у нас с одной стороны наши пользователи, есть у нас данные в S3 bucket-е и есть промежуточный CloudFront.

00:01:51.440 --> 00:02:02.240

Это наш CDN, Content Delivery Network, который позволяет доставлять ваши данные из S3 bucket-а до ваших клиентов по всему миру с меньшими задержками.

00:02:02.240 --> 00:02:16.440

Таким образом, у пользователей есть возможность обращаться напрямую к S3, это будет медленнее, но есть такая возможность, а также есть возможность обращаться через CloudFront, это будет быстрее.

00:02:16.440 --> 00:02:38.760

Что необходимо вам сделать в рамках задания, это дать возможность только специфичному клиенту обращаться через CloudFront к вашим данным в S3 и запретить пользователю обращаться к данным в S3 напрямую.

00:02:38.760 --> 00:02:49.080

Для этого существует два отдельных функционала.

00:02:49.080 --> 00:03:10.520

Для того, чтобы запретить прямой доступ к S3, необходимо настроить Origin Access Identity, OAI, так чтобы только у CloudFront Distribution была возможность обращаться к данным в S3, для всех остальных внешних обращений к S3 данным доступ будет запрещен.

00:03:10.520 --> 00:03:14.320

Это первый вариант, правильный вариант ответа.

00:03:14.320 --> 00:03:28.200

Если мы говорим про второй, необходимо на уровне CloudFront настроить так называемые Signed URL или Signed Cookies, которые предоставляют выборочный доступ для клиентов, пользователей вашего приложения.

00:03:28.200 --> 00:03:44.360

В первом случае, когда мы говорим про Signed URL, генерируется специальная ссылка, у нее есть время жизни, есть policy, в котором прописано кому и как вы предоставляете доступ.

00:03:44.360 --> 00:03:54.560

Передав эту ссылку, все ваши клиенты и пользователи с этой ссылкой могут без каких-либо препятствий обращаться к вашим данным.

00:03:54.560 --> 00:04:05.360

У всех других, у которых есть старая ссылка, но при этом не прописаны некоторые данные, касающиеся Signed URL, доступ будет запрещен.

00:04:05.360 --> 00:04:09.840

То же самое относится к Signed Cookies, работает немного по-другому.

00:04:09.840 --> 00:04:33.600

Идея в том, что вы при обращении к странице для ваших пользователей в их браузерах для вашего сайта, прописываете некоторые cookies и в момент обращения проверяете есть ли нужные вам cookies и есть ли необходимые правильные значения у этих cookies.

00:04:33.600 --> 00:04:43.080

Если все совпадает, все отлично, доступ предоставляется и по прямой ссылке пользователи могут дальше продолжать обращаться к вашим данным.

00:04:43.080 --> 00:04:51.960

Для всех других пользователей, у которых нет необходимых cookies файлов, они получат сообщение об ошибке, что доступ запрещен.

00:04:51.960 --> 00:04:59.560

Давайте теперь подробнее остановимся на неверных вариантах.

00:04:59.560 --> 00:05:03.280

Первый неверный вариант упоминает сервис AWS App Mesh.

00:05:03.280 --> 00:05:17.960

В этом случае он нам не подходит, так как App Mesh это тот сервис, который предоставляет нам возможность удобного networking-а на уровне наших приложений.

00:05:17.960 --> 00:05:22.120

Когда мы говорим про AWS Cloud Map, аналогичный сервис.

00:05:22.120 --> 00:05:30.800

Идея в том, что в Cloud Map мы храним название и расположение наших приложений, ресурсов, компонентов.

00:05:30.800 --> 00:05:40.000

И таким образом это центральное место, куда другие ваши приложения, компоненты могут обращаться для поиска других частей вашей IT инфраструктуры.

00:05:40.000 --> 00:05:47.560

Если мы говорим про третий неверный вариант, он в теории мог бы быть верным, если бы не ограничение в вопросе.

00:05:47.560 --> 00:05:57.520

В вопросе сказано, что мы должны передавать приватный контент через CloudFront для того, чтобы обезопасить распространение наших данных.

00:05:57.520 --> 00:05:59.720

Поэтому этот вариант не подходит.

00:05:59.720 --> 00:06:02.080

Давайте подробнее расскажу о нем.

00:06:02.080 --> 00:06:17.120

Здесь упоминается, что мы могли бы настроить S3 Pre-signed URL и через нее предоставлять доступ клиентам, а также для S3 запретить доступ ко всем остальным источникам.

00:06:17.120 --> 00:06:25.200

В этом случае запрещается в том числе доступ для CloudFront и через CloudFront уже обслуживать трафик к S3 не получится.

00:06:25.200 --> 00:06:37.360

Более того, у вас может начаться путаница, что здесь Pre-signed URL, чуть выше мы говорили про signed URL на уровне CloudFront.

00:06:37.360 --> 00:06:38.360

Да, так и есть.

00:06:38.360 --> 00:06:43.480

Pre-signed URL доступен как для S3, так и для CloudFront.

00:06:43.480 --> 00:06:46.120

На стороне CloudFront это более продвинутое решение.

00:06:46.120 --> 00:06:59.640

Более того, на стороне CloudFront можно настроить Signed Cookies и в целом функционал при работе с CloudFront намного продвинутый.

00:06:59.640 --> 00:07:13.200

Исходя из ограничений вопроса, таким образом мы говорим, что этот вариант ответа является неверным.

00:07:13.200 --> 00:07:15.720

На этом мы разобрали вопрос Practice Test-а.

00:07:15.720 --> 00:07:22.720

Спасибо за внимание.