WEBVTT

00:00:00.000 --> 00:00:06.000

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

00:00:08.000 --> 00:00:17.000

Что дано? Компания планирует хранить некоторые конфиденциальные данные по налогам в AWS.

00:00:18.000 --> 00:00:22.000

Эти данные не должны быть доступны публично.

00:00:22.000 --> 00:00:29.000

Более того, доступ к этим данным должен быть доступным только для определенного VPC.

00:00:31.000 --> 00:00:44.000

Второе требование. Нам необходимо обеспечить, что объекты в этом хранилище должны быть защищены от удаления и перезаписи.

00:00:44.000 --> 00:00:53.000

Таким образом, должно сохраняться регуляторное требование WORM, то есть write-once-read-many.

00:00:54.000 --> 00:01:02.000

Идея в том, что записывается один раз и может считываться много раз. Перезаписываться эти объекты тоже не могут.

00:01:02.000 --> 00:01:13.000

Нам необходимо из предложенных вариантов ответа выбрать два варианта ответа, которые помогают это требование реализовать.

00:01:15.000 --> 00:01:19.000

Давайте посмотрим, какие варианты ответов нам даны.

00:01:20.000 --> 00:01:25.000

Мы видим, что первый и четвертый варианты ответов являются правильными.

00:01:25.000 --> 00:01:32.000

Более того, мы видим, что ни один из вариантов не похож на другой.

00:01:33.000 --> 00:01:41.000

Таким образом, этот вопрос является достаточно сложным, требует знания нескольких особенностей AWS.

00:01:42.000 --> 00:01:49.000

Давайте попробуем разобрать каждый из вариантов ответа и дать ответ, почему оно верное или неверное.

00:01:49.000 --> 00:01:56.000

Давайте вспомним теорию, а именно функционал Access Points сервиса Amazon S3.

00:01:57.000 --> 00:02:09.000

Это тот функционал, который позволяет ограничить доступ к S3 Bucket на операции с объектами, такие как чтение объекта либо запись объекта.

00:02:09.000 --> 00:02:21.000

Вы можете видеть на картинке, в левом навигационном меню было выбрано Access Points сервиса Amazon S3 и указываются некоторые входные данные, а именно Bucket.

00:02:22.000 --> 00:02:31.000

Далее указывается список VPC, на которые ставится ограничение.

00:02:31.000 --> 00:02:39.000

Из всех других не указанных VPC к этому S3 обратиться будет невозможно.

00:02:39.000 --> 00:02:48.000

Другой момент это то, что Access Points хорош тем, что не требует выхода в интернет.

00:02:48.000 --> 00:02:54.000

Все операции обмена данными происходят внутри глобальной инфраструктуры AWS.

00:02:54.000 --> 00:03:04.000

Это все дает дополнительные возможности, а именно то, что мы можем настроить cross-regional доступ к вашему S3 Bucket через Access Points.

00:03:04.000 --> 00:03:15.000

Это также возможно. В этом случае используется AWS Global Accelerator, который помогает быстрее передавать ваши данные.

00:03:15.000 --> 00:03:24.000

Другой функционал, который важен для решения конкретной задачи, это S3 Object Lock.

00:03:24.000 --> 00:03:39.000

Идея в том, что этот функционал запрещает запись и перезапись объектов внутри нашего S3 Bucket и дает возможность бесконечное количество раз эти объекты считывать.

00:03:39.000 --> 00:03:48.000

Есть определенные нюансы. Object Lock настраивается в момент создания S3 Bucket.

00:03:48.000 --> 00:03:58.000

Таким образом, в момент создания вам необходимо в Advanced Settings для опции Object Lock выбрать опцию Enable.

00:03:58.000 --> 00:04:04.000

Обратите внимание, что когда вы включаете Object Lock, его после отключить будет невозможно.

00:04:05.000 --> 00:04:10.000

Более того, он автоматически включает Bucket Versioning.

00:04:11.000 --> 00:04:17.000

Когда у нас включенный Object Lock, Bucket Versioning отключен или остановлен быть не может.

00:04:17.000 --> 00:04:31.000

Таким образом, правильными ответами являются использование Amazon S3 Access Point для того, чтобы ограничить доступ на конкретный VPC.

00:04:32.000 --> 00:04:54.000

И второй вариант ответа - это использовать функционал Object Lock во время создания S3 Bucket, для того, чтобы учитывалось регуляторное требование записывать файлы один раз и иметь возможность считывать эти файлы необходимое количество раз.

00:04:56.000 --> 00:05:01.000

Давайте теперь подробнее остановимся на вариантах ответов, которые являются неверными.

00:05:01.000 --> 00:05:10.000

В первом случае говорится про AWS Network Firewall. Network Firewall настраивается на уровне VPC, не на уровне S3 Bucket.

00:05:11.000 --> 00:05:19.000

Таким образом, даже если мы можем настроить поток данных для VPC, ограничить доступ к S3 Bucket через Network Firewall мы не можем.

00:05:20.000 --> 00:05:22.000

Поэтому этот вариант является неверным.

00:05:22.000 --> 00:05:35.000

Если мы говорим про вариант S3 Glacier, он также не подходит, потому что Glacier используется для хранения архивных данных и извлечения данных не сразу, а через какое-то время.

00:05:36.000 --> 00:05:46.000

Нам же сказано, что мы должны иметь возможность при необходимости в ту же секунду извлекать эти данные.

00:05:46.000 --> 00:05:54.000

Другой момент это то, что Glacier не запрещает перезаписывать или создавать новые файлы.

00:05:55.000 --> 00:06:02.000

Таким образом, требование WORM, то есть write-once-read-many не выполняется.

00:06:02.000 --> 00:06:24.000

Если мы говорим про последний вариант с включением опции Object Lock при этом отключить Object Versioning, он сам себя исключает, потому что в момент, когда вы включаете Object Lock, автоматически включается Object Versioning.

00:06:25.000 --> 00:06:30.000

Его вы отключить или даже остановить после включения опции Object Lock не можете.

00:06:30.000 --> 00:06:33.000

Поэтому этот вариант является неверным.

00:06:33.000 --> 00:06:39.000

На этом мы разобрали вопрос Practice Test-а. Спасибо за внимание.