WEBVTT

00:00:00.000 --> 00:00:04.000

Добрый день, уважаемые студенты.

00:00:04.000 --> 00:00:09.000

Мы с вами начинаем разбор вопроса Practice Test-а.

00:00:09.000 --> 00:00:37.080

Согласно вопросу, компания решила сделать расчет и через сервис Total Cost of Ownership посчитала и сравнила использование Amazon S3 либо использование локального дата-центра для хранения персональных данных 1200 работников компании.

00:00:37.080 --> 00:00:51.120

Согласно расчетам, компания решила, что использование Amazon S3 будет выгодным решением и попросила вас как Solutions Architect определить шаги, которые необходимо предпринять.

00:00:51.120 --> 00:00:56.120

Есть некоторые моменты, которые нужно учитывать.

00:00:56.120 --> 00:01:04.480

Первое - мы должны осуществить Single sign-on, то есть SSO.

00:01:04.480 --> 00:01:15.360

Все сотрудники должны иметь возможность, используя рабочий логин-пароль, авторизовываться в Amazon S3.

00:01:15.360 --> 00:01:27.520

Далее, необходимо использовать существующие Active Directory AD или LDAP, в котором хранится список всех ваших сотрудников.

00:01:27.520 --> 00:01:39.600

А также необходимо обеспечить разграничение данных, так чтобы персональные данные одного сотрудника не были видны другому сотруднику.

00:01:39.600 --> 00:01:51.360

Из предложенных вариантов необходимо выбрать два варианта, которые помогают это осуществить.

00:01:51.360 --> 00:01:54.040

Здесь вы видите все варианты ответов.

00:01:54.040 --> 00:01:57.960

Также видите, что 3 и 5 варианты ответа являются верными.

00:01:57.960 --> 00:02:08.360

Все варианты ответов отличаются друг от друга, поэтому можно утверждать, что сложность вопроса выше среднего.

00:02:08.360 --> 00:02:21.600

Давайте разберем каждый вариант ответа и попробуем ответить на вопрос, почему он является верным или неверным.

00:02:21.600 --> 00:02:26.160

Для того, чтобы лучше понять, что от нас требуется, обратите внимание на диаграмму.

00:02:26.160 --> 00:02:40.200

В диаграмме с левой стороны видите организацию, в которой есть сотрудники и Identity provider корпоративный, который хранит учетные записи пользователей, в том числе связки, логин и пароль.

00:02:40.200 --> 00:02:47.360

С правой стороны видите AWS и сервис Amazon S3, который хранит все данные ваших сотрудников.

00:02:47.360 --> 00:02:58.560

Нам необходимо, чтобы сотрудники, могли, используя корпоративный логин и пароль, обращаться к данным в S3.

00:02:58.560 --> 00:03:02.240

Для этого следует выполнить следующие шаги.

00:03:02.240 --> 00:03:09.600

Для пользователей эти шаги прозрачны, они получают прямой доступ к S3 bucket.

00:03:09.600 --> 00:03:12.760

На фоне происходят следующие действия.

00:03:12.760 --> 00:03:20.840

Первым делом, когда сотрудник вводит логин и пароль, эта связка идет к корпоративному Identity provider.

00:03:20.840 --> 00:03:26.880

Оно подтверждает, что действительно эта связка верная, и доступ запрашивает наш сотрудник.

00:03:26.880 --> 00:03:37.560

Как только это подтверждается, далее запрос уходит на сервис AWS STS, который предоставляет нам роль и временный доступ.

00:03:37.560 --> 00:03:45.360

Используя эту роль, можно уже обращаться к различным сервисам на стороне AWS, в нашем случае это S3.

00:03:45.360 --> 00:03:56.200

Далее мы можем настроить Identity-Based Policy на уровне нашей роли, либо можем настроить Bucket Policy на уровне S3 bucket.

00:03:56.200 --> 00:04:09.760

Благодаря этим Policy мы можем ограничить доступ одному сотруднику на файлы другого сотрудника.

00:04:09.760 --> 00:04:15.200

Давайте теперь рассмотрим неправильные варианты ответов и почему они таковыми являются.

00:04:15.200 --> 00:04:36.440

Вариант ответа, где предлагается использовать OKTA, OneLogin или любой другой сторонний SSO решение, оно заведомо неверное, потому что в вопросе нам уже было сказано использовать корпоративный Active Directory AD или LDAP, то есть корпоративные охранилища учетных записей сотрудников.

00:04:36.440 --> 00:04:38.400

Этот вариант является неверным.

00:04:38.400 --> 00:05:07.240

Тот вариант, где предлагается использовать WorkDocs, также является не совсем верным. Потому что WorkDocs - это SaaS решение, готовое решение. Когда вы работаете с WorkDocs вы с S3 взаимодействовать не можете, соответственно ограничение, которое вы хотели выставить на уровне сотрудников, вы сделать с WorkDocs не сможете и поэтому этот вариант является неверным.

00:05:07.240 --> 00:05:40.880

Последний вариант, где предлагается создать 1200 IAM пользователей, является также неверным, так как нет необходимости создавать такое большое количество IAM пользователей, а достаточно интегрироваться с существующим хранилищем учетных записей, именно AD и LDAP в вашей компании и достаточно использовать правильно написанную роль.

00:05:40.880 --> 00:05:45.280

На этом мы разобрали вопрос Practice Test-а.

00:05:45.280 --> 00:06:08.720

Спасибо за внимание.