Люсин Дмитрий Витальевич 409038

Рубежная работа №1 – Вариант 1

Зачем в облаке предусмотрено столько регионов? Зачем там кроме регионов еще и зоны?

Сам по себе регион – это физическое местоположение, в котором располагается оборудование в дата-центрах. Так зачем же предусматривать большое количество регионов?

- **Производительность:**

Повсеместно «создавая» регионы, работа с данными для пользователя становится проще и быстрее. Ведь куда проще работать с данными из того региона, который ближе к потенциальному пользователю. Также каждый регион имеет своё оборудование, которое не зависит от других регионов

- **Безопасность:**

Как было сказано в предыдущем пункте, регионы независимы друг от друга, поэтому если в одном из регионов происходит сбой по какой-либо причине, то другие регионы продолжают функционировать. Это позволяет предотвратить глобальные сбои в работе регионов.

- **¿Законы?:**

Каждая страна (или блок стран) имеет своё законодательство, в котором предусмотрены требования к хранению и реализации данных. Регионы как раз позволяют облегчить выполнение данных требований

И вот теперь перейдём к зонам доступности. Зона доступности – это физический дата-центр (или группа дата-центров). Если говорить о причинах размещения нескольких зон в общем плане, то они в большенстве своём такие же, как и у регионов: Производительность (каждая зона – отдельный дата-центр со своим независимым оборудованием и всем остальным) и Безопасность (в случае выхода из строя одной зоны, другие продолжают функционировать).

В общей сложности можно сказать, что регионы предназначаются для работы на глобальном уровне, а зоны доступности – на локальном уровне

Рубежная работа №2 – Вариант 7

Поговорим про безопасность. Какие существуют направления повышения безопасности в облаке? Какие компоненты безопасности настраивать обязательно?

Направления безопасности:

• **Безопасный доступ и управление идентификацией:**

Здесь основой служит IAM – специальный инструмент, который предоставляется поставщикам облачных услуг и позволяет пользователям управлять аутентификацией и различными расширениями. IAM позволяет создавать отдельные учётные записи и защищать их многофакторной аутентификацией

• **Шифрование данных:**

Процесс защиты данных, во время которого данные кодируются в зашифрованный текст. Управление происходит благодаря управляющим ключам (KMS).

• **Управление уязвимостями:**

Процесс выявления, информирования и устранения рисков безопасности. Суть сводится к частому сканированию системы на предмет угроз безопасности с последующим их устранением.

• **Резервное копирование и восстановление данных:**

Процесс создания резервных копий всех данных на дополнительный носитель (локальный или облачный). Например возможно использование AWS Backup. Само собой все резервные копии данных также защищены шифрованием

• **Реагирование на инцидент:**

Процесс работы команд специалистов по быстрому устранению неожиданно возникших сбоев в работе системы. Помимо быстрого устранения угрозы и минимизации потенциального ущерба включает в себя разработку планов на реагирование. Для анализа, разработки и улучшения планов необходимо сохранять данные об инцидентах

• **Сегментация сетей:**

Процесс разделения компьютерной сети на более мелкие изолированные сегменты. В дополнение имеется возможность использования виртуальных частных сетей (VPS). Сюда же входит обязательная необходимость настройки межсетевого экрана (firewall), в следствии чего появляется возможность ограничения доступа к критически важным ресурсам. Соответственно необходима защита от DDoS-атак

Если говорить об обязательных компонентах безопасности, то:

• В дополнение к пункту о безопасном доступе и идентификации можно дополнить о возможности проводить аудит и удаление неиспользуемых учётных записей

• В дополнение к пункту о шифровании можно добавить возможность шифрование при передаче данных с использованием SSL/TLS, а также регулярное обновление ключей шифрования

• Для защиты веб-приложений необходимо настраивать WAF. Также стоит использовать безопасные инфраструктуры, например AWS CloudFormation

• В дополнение к пункту об управлении уязвимостями можно добавить настройку логирования всех происходящих операций. Также помимо сканирования необходимо настроить систему оповещения о подозрительной активности, например с использованием SIEM-системы