Шифрование данных в AWS

SOFTPROM
softprom.com • info@softprom.com

amazon web services | Partner Network
ADVANCED CONSULTING PARTNER

2020

Шифрование данных в AWS

Поддерживать доверие клиентов – неизменный приоритет Amazon Web Services (AWS). AWS информирует своих клиентов о политиках защиты конфиденциальности и безопасности данных, а также о применяемых методах и технологиях. AWS берет на себя следующие обязательства и предоставляет следующие возможности.

Доступ. Клиент берет управление своим контентом полностью в свои руки и несет ответственность за настройку доступа к сервисам и ресурсам AWS. Для эффективного выполнения этой задачи AWS предоставляет расширенный набор инструментов для управления доступом, шифрования и ведения журналов (например, AWS Identity and Access Management, AWS Organizations и AWS CloudTrail). Кроме того, AWS предоставляет API для настройки управления разрешениями доступа к любым сервисам, которые клиенты разрабатывают или разворачивают в среде AWS. AWS не получает доступ к контенту клиентов и не использует его для каких-либо целей без соответствующего согласия. AWS ни при каких обстоятельствах не использует контент клиентов или связанную с ним информацию в маркетинговых и рекламных целях.

Хранение. Клиенты выбирают регионы AWS для хранения своего контента, а также тип хранилища. Клиенты могут реплицировать контент между регионами AWS и создавать резервные копии в нескольких регионах. AWS не будет перемещать или реплицировать контент за пределы выбранных клиентом регионов AWS без согласия клиента, за исключением отдельных случаев, когда это требуется законодательством или обязывающим предписанием государственного органа.

Безопасность. Клиенты выбирают способы защиты контента. AWS предлагает надежные средства шифрования контента при передаче и хранении, а также предоставляет клиентам возможность использовать собственные ключи шифрования. Новые возможности.

- Функции шифрования данных, доступные в сервисах AWS для хранилищ и баз данных, таких как Amazon Elastic Block Store, Amazon Simple Storage Service, Amazon Relational Database Service и Amazon Redshift.
- Гибкие варианты управления ключами, включая AWS Key Management Service (KMS), позволяющие клиентам выбирать, сохранять ли полный контроль над ключами шифрования или передать управление ключами AWS.
- Клиенты AWS могут обеспечить шифрование на стороне сервера (SSE) с помощью ключей, управляемых Amazon S3 (SSE-S3) или AWS KMS (SSE-KMS), либо с помощью собственных ключей (SSE-C).

Раскрытие контента клиентов. AWS ни при каких условиях не раскрывает контент клиентов, кроме случаев, когда это требуется законодательством или постановлением обязательного характера, выпущенным государственным органом. Если государственный орган направляет в AWS требование предоставить контент клиента, AWS всегда предлагаем им обратиться за этими данными непосредственно к клиенту. Если AWS будет вынужден раскрыть контент клиента государственному органу, клиенту направляется обоснованное уведомление об этом требовании, чтобы он мог

подготовить охранный судебный приказ или другой инструмент правовой защиты, если AWS имеет на это законное право.

Гарантия безопасности. Опираясь на международные рекомендации по защите данных и конфиденциальности, в AWS разработали программу обеспечения безопасности, которая помогает клиентам безопасно работать в AWS и в полной мере использовать нашу среду управления безопасностью. Процессы обеспечения безопасности в AWS и управления ею были неоднократно проверены независимыми сторонними специалистами.

Как AWS классифицирует данные клиентов

В AWS данные клиентов подразделяются на две категории: контент клиента и данные аккаунта.

К контенту клиента относится программное обеспечение (включая образы машин), данные, текстовые, аудио- и видеофайлы, файлы изображений, которые клиент или любой конечный пользователь перемещает в нашу систему для обработки, хранения или размещения с помощью сервисов AWS в рамках аккаунта клиента, а также любые результаты вычислений, которые клиент или любой конечный пользователь получает в результате использования сервисов AWS. Например, контент клиента включает любую информацию, которую клиент или конечные пользователи хранят в Amazon Simple Storage Service (S3). Контент клиента не включает данные аккаунта. Они будут описаны ниже. К контенту клиента применяются условия Пользовательского соглашения AWS и Условия обслуживания AWS.

Данные аккаунта – это информация о клиенте, которую он предоставляет для создания или администрирования своего аккаунта. Данные аккаунта включают, например, личные имена, имена пользователей, телефонные номера, адреса электронной почты и информацию об оплате, связанные с аккаунтом клиента. К данным аккаунта применяются методы работы с информацией, описанные в Заявлении AWS о защите конфиденциальности.

Соответствие стандартам

Amazon Web Services (AWS) позволяет клиентам шифровать данные с помощью сервисов шифрования данных при передаче, соответствующих требованиям FIPS 140-2, и шифрования данных при хранении согласно стандарту FIPS-197.

AWS Key Management Service (KMS) позволяет без труда создавать криптографические ключи для всех процессов шифрования и использования их в приложениях и различных сервисах AWS, а также управлять этими ключами.

Сервис AWS KMS отличается надежностью и отказоустойчивостью, он использует для защиты ключей аппаратные модули безопасности, проверенные или находящиеся в процессе проверки на соответствие стандарту FIPS 140-2. Эти ключи никогда не покидают пределы аппаратных модулей безопасности сервиса AWS KMS,

соответствующих требованиям FIPS, в незашифрованном виде и не передаются персоналу AWS.

AWS KMS интегрирован с AWS CloudTrail и предоставляет журналы использования ключей для обеспечения соответствия нормативным требованиям.

Средства управления безопасностью и качеством сервиса AWS KMS были подтверждены и сертифицированы по следующим схемам соответствия требованиям.

- Отчеты о соответствии AWS требованиям Service Organization Controls (SOC 1, SOC 2 и SOC 3). Загрузить копию этих отчетов можно в AWS Artifact.
- PCI DSS Level 1. Подробнее о соответствии сервисов AWS стандарту PCI DSS см. на странице вопросов и ответов по PCI DSS.
- FIPS 140-2. Все криптографические модули AWS KMS уже проверены или проверяются на соответствие стандарту FIPS 140-2 Level 2, а по некоторым аспектам, включая физическую защиту, на соответствие уровню Level 3. Подробные сведения можно найти в сертификате FIPS 140-2 для модулей HSM сервиса AWS KMS и в соответствующей политике безопасности.
- FedRAMP. Подробнее о соответствии AWS требованиям FedRAMP см. на странице соответствия требованиям FedRAMP.
- HIPAA. Подробнее см. на странице соответствия требованиям HIPAA.

Список сервисов AWS, подпадающих под действие программы обеспечения соответствия стандартам

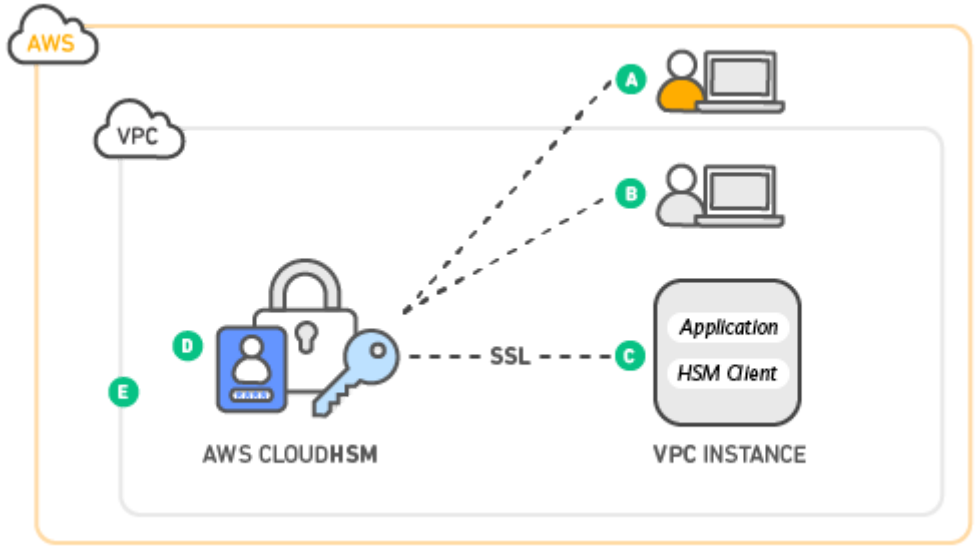
Собственное хранилище ключей

AWS KMS позволяет создать собственное хранилище ключей, используя управляемые клиентом модули HSM. Для каждого собственного хранилища ключей кластер AWS CloudHSM создает резервную копию. Когда вы создаете Customer Master Key (CMK) в собственном хранилище ключей, сервис генерирует материалы ключей и сохраняет их в кластере AWS CloudHSM, который находится под вашим полным управлением. Когда вы применяете CMK из собственного хранилища ключей, все криптографические операции с этим ключом выполняются в вашем кластере AWS CloudHSM.

CMK, сохраненные в собственном хранилище ключей и управляемые вами, как и любые другие CMK, можно использовать в любом сервисе AWS, который поддерживает интеграцию с AWS KMS.
Использование собственного хранилища ключей влечет за собой дополнительные расходы на кластер AWS CloudHSM. Ответственность за доступность материала ключей в этом кластере несет сам клиент.

AWS CloudHSM – это облачный аппаратный модуль безопасности (HSM), который позволяет без труда генерировать и использовать в облаке AWS собственные ключи шифрования. С помощью CloudHSM можно управлять собственными ключами шифрования, используя модули HSM, проверенные на соответствие стандарту FIPS 140-2 Level 3. CloudHSM обеспечивает гибкость интеграции с приложениями с

помощью стандартных API-интерфейсов, таких как PKCS#11, Java Cryptography Extensions (JCE) и библиотеки Microsoft CryptoNG (CNG).



AWS CloudHSM работает в клиентском облаке Amazon Virtual Private Cloud (VPC), что позволяет без труда использовать модули HSM с приложениями, запущенными на инстансах Amazon EC2. При работе с CloudHSM можно использовать стандартные средства управления безопасностью облака VPC для управления доступом к модулям HSM. Приложения клиента подключаются к модулям HSM, используя SSL-каналы с двусторонней аутентификацией, установленные клиентским ПО HSM. Поскольку модули HSM находятся в ЦОД Amazon рядом с инстансами EC2, можно уменьшить сетевые задержки между приложениями и модулями HSM по сравнению с использованием локальных модулей HSM.

A. AWS управляет модулем аппаратного обеспечения безопасности (HSM), но не имеет доступа к ключам клиента.
B. Пользователь контролирует собственные ключи и управляет ими.
C. Производительность приложения улучшается (вследствие непосредственной близости к рабочим нагрузкам AWS).
D. Ключи безопасно хранятся в защищенных от взлома аппаратных модулях в нескольких зонах доступности (AZ).
E. Модули HSM находятся в облаке Virtual Private Cloud (VPC) и изолированы от других сетей AWS.

В архитектуре сервиса AWS CloudHSM предусмотрены разделение обязанностей и контроль доступа на основе ролей. AWS осуществляет мониторинг работоспособности и сетевой доступности модулей CloudHSM, но не имеет отношения к созданию данных ключей, хранящихся в модуле HSM, или к управлению ими. Клиент управляет модулями HSM, генерирует и использует свои ключи шифрования.

Асимметричные ключи

AWS KMS предоставляет возможность создавать и использовать асимметричные CMK и пары ключей данных. Вы можете назначить CMK для использования в роли пары ключей подписывания или шифрования. Генераций пар ключей и асимметричные криптографические операции с такими CMK выполняются в аппаратных модулях HSM.

Вы можете запросить открытую часть асимметричного CMK для использования в локальных приложениях, а закрытая часть никогда не покидает пределов сервиса. Вы также может создать с помощью сервиса асимметричную пару ключей данных. Такая операция возвращает копию открытого и закрытого ключей в формате обычного текста, а также копию закрытого ключа, зашифрованную предоставленным вами симметричным CMK. Версии ключей в формате обычного текста вы можете использовать в локальном приложении, а зашифрованную копию закрытого ключа сохранить отдельно для использования в будущем.

Перечень упомянутых сервисов AWS

Пример использования	Сервис AWS
Хранение ключей и управление ими	AWS Key Management Service (KMS)
Аппаратное хранилище ключей для соответствия нормативным требованиям	AWS CloudHSM
Ротация и извлечение конфиденциальных данных, а также управление ими	AWS Secrets Manager
Безопасное управление доступом к сервисам и ресурсам	AWS Identity & Access Management (IAM)
Бесплатный портал самообслуживания для доступа по требованию к отчетам AWS о соответствии требованиям	AWS Artifact