Стандарт безопасности данных индустрии платежных карт (PCI DSS) в AWS

SOFTPROM
softprom.com • info@softprom.com

amazon web services | Partner Network
ADVANCED CONSULTING PARTNER

2020

Стандарт безопасности данных индустрии платежных карт (PCI DSS) в AWS

Стандарт безопасности данных индустрии платежных карт (Payment Card Industry Data Security Standard - PCI DSS) – это проприетарный стандарт в области информационной безопасности. Он находится под административным управлением Совета по стандартам безопасности данных индустрии платежных карт, основанного компаниями American Express, Discover Financial Services, JCB International, MasterCard Worldwide и Visa Inc.
Стандарт PCI DSS распространяется на юридические лица, которые занимаются хранением, обработкой или передачей данных владельцев карт (CHD) или конфиденциальных данных аутентификации (SAD), в том числе на торговые компании, процессинговые центры, эквайеров, эмитентов карт и поставщиков услуг. Стандарт PCI DSS утверждается платежными системами, а его администрированием занимается Совет по стандартам безопасности данных индустрии платежных карт. Сертификат соответствия требованиям (AOC) PCI DSS и обзор сферы ответственности можно получить с помощью AWS Artifact, портала самообслуживания для доступа по требованию к отчетам AWS по соответствию требованиям. Войдите в раздел AWS Artifact в Консоли управления AWS или см. подробности на странице Начало работы с AWS Artifact.

Amazon Web Services (AWS) является сертифицированным поставщиком услуг PCI DSS Level 1 – самого высокого уровня оценки из существующих. Оценка соответствия проводилась компанией Coalfire Systems Inc., независимым квалифицированным инспектором безопасности (QSA). Сертификат соответствия требованиям (AOC) PCI DSS и обзор сферы ответственности можно получить с помощью AWS Artifact, портала самообслуживания для доступа по требованию к отчетам AWS по соответствию требованиям. Войдите в раздел AWS Artifact в Консоли управления AWS или см. подробности на странице Начало работы с AWS Artifact.

Перечень сервисов AWS, соответствующих требованиям PCI DSS, см. на вкладке PCI на странице Сервисы AWS в программе обеспечения соответствия.

При использовании сервисов AWS для хранения, обработки и передачи данных владельцев платежных карт ***вы можете полагаться на технологическую инфраструктуру AWS в ходе прохождения собственной сертификации на соответствие требованиям PCI DSS.***
AWS не занимается непосредственным хранением, передачей или обработкой данных владельцев карт для своих клиентов. Однако с помощью сервисов AWS клиенты могут создавать собственные среды для данных платежных карт, в которых будут

происходить процессы хранения, передачи или обработки данных владельцев платежных карт.

Даже если у вас нет сертификации PCI DSS, соответствие наших сервисов требованиям PCI демонстрирует приверженность AWS информационной безопасности на всех уровнях. Поскольку соответствие стандарту PCI DSS проверяется независимой сторонней компанией, это означает, что наша программа управления безопасностью является всесторонней и соответствует передовым отраслевым практикам.

Клиенты должны проходить собственную сертификацию на соответствие требованиям PCI DSS, поэтому для подтверждения того, что конкретная среда удовлетворяет всем требованиям PCI DSS, может потребоваться дополнительное тестирование. Однако в отношении среды для работы с данными владельцев карт (CDE), развернутой на AWS, квалифицированный инспектор безопасности (QSA) может положиться на сертификат соответствия (AOC), полученный AWS, без дополнительного тестирования.

Пакет по соответствию AWS требованиям PCI включает:

- сертификат соответствия AWS требованиям PCI DSS 3.2.1 (AOC);
- Обзор сферы ответственности AWS по обеспечению соответствия требованиям PCI DSS 3.2.1.

AWS входит в глобальный реестр поставщиков услуг Visa и в список одобренных поставщиков услуг MasterCard. Эти списки поставщиков услуг еще раз демонстрируют, что AWS успешно прошла сертификацию на соответствие требованиям PCI DSS и удовлетворяет всем применимым программным требованиям Visa и MasterCard.

Платформа AWS – это виртуальная многопользовательская среда. ***В AWS реализованы эффективные процессы управления безопасностью, соответствия требованиями PCI DSS и другие средства управления, которые безопасно изолируют клиентов в собственных защищенных средах***. Эта безопасная архитектура была протестирована независимым инспектором QSA, который установил, что она соответствует всем применимым требованиям стандарта PCI DSS.
Совет по стандартам безопасности PCI опубликовал документ PCI DSS Cloud Computing Guidelines для клиентов, поставщиков услуг и проверяющих в сфере облачных вычислительных сервисов. В нем описаны возможные модели сервисов и распределение между поставщиками и клиентами ролей и обязанностей в части обеспечения соответствия требованиям.

Сертификат соответствия, выданный AWS – это показатель всесторонней оценки методов управления физической безопасностью в ЦОД AWS. QSA торговой компании может не проводить проверку безопасности ЦОД AWS.

AWS не считается "Поставщиком совместно используемого хостинга" по стандарту PCI-DSS. Поэтому требование DSS A1.4 неприменимо. Согласно

нашей Модели общей ответственности мы предоставляем пользователям возможность проводить следственные мероприятия в собственной среде AWS без дополнительной помощи со стороны AWS. Эта возможность обеспечивается через сервисы AWS и сторонние решения, доступные на AWS Marketplace. Дополнительные сведения см. в следующих ресурсах.

- Упрощение реагирования на инциденты безопасности и следственные мероприятия в AWS
- Руководство по реагированию на инциденты безопасности AWS

Если используемые сервисы AWS соответствуют требованиям PCI DSS, вся инфраструктура, поддерживающая соответствующие сервисы, удовлетворяет требованиям. Отдельной среды или специального API нет. Любой сервер или объект данных, который развернут в этих сервисах или использует их, находится в среде, соответствующей требованиям PCI DSS, независимо от региона. Перечень сервисов AWS, соответствующих требованиям PCI DSS, см. на вкладке PCI на странице Сервисы AWS в программе обеспечения соответствия.

Многие клиенты уже выполнили развертывание в AWS сред для обслуживания владельцев карт (полное или частичное) и успешно сертифицировали эти среды. AWS не раскрывает информацию о клиентах, прошедших сертификацию PCI DSS, но регулярно сотрудничает с клиентами и организациями, выполняющими их оценку на соответствие PCI DSS, в вопросах планирования, развертывания, сертификации и выполнения ежеквартального анализа среды обработки информации о владельцах карт на AWS.

Существует два основных подхода к ежегодному подтверждению соответствия требованиям PCI DSS. Первый – поручить внешнему квалифицированному инспектору безопасности (QSA) провести оценку связанных частей среды и представить отчет о соответствии требованиям (ROC) и сертификат соответствия (AOC). Такой подход чаще применяется организациями, которые обрабатывают большие объемы транзакций. ***Второй*** – заполнить анкету самооценки (SAQ). Этот подход обычно применяется организациями, которые обрабатывают меньшие объемы транзакций.
Важно помнить, что ответственность за поддержание соответствия требованиям несут платежные системы и эквайеры, а не Совет по стандартам безопасности PCI.

Ниже приведен краткий обзор требований PCI DSS.

Создание и поддержка безопасных сетей и систем.	1. Установка и поддержка настроек брандмауэра, необходимых для защиты данных владельцев карт. 2. Замена установленных на заводе системных паролей и прочих параметров безопасности по умолчанию.
Защита данных владельцев карт.	3. Защита данных владельцев карт при хранении. 4. Шифрование данных владельцев карт при передаче по открытым публичным сетям.

Реализация программы контроля уязвимости.	5. Защита всех систем от вредоносного ПО и регулярное обновление антивирусных программ. 6. Разработка и поддержка безопасных систем и приложений.
Реализация строгих мер контроля доступа.	7. Ограниченный доступ к данным владельцев карт, строго в рамках практической необходимости. 8. Идентификация и аутентификация доступа к компонентам системы. 9. Ограничение физического доступа к данным владельцев карт.
Регулярный мониторинг и тестирование сетей.	10. Идентификация и мониторинг всех обращений к сетевым ресурсам и данным владельцев карт. 11. Регулярное тестирование систем и процессов, связанных с безопасностью.
Обеспечение политики информационной безопасности.	12. Обеспечение политики информационной безопасности в отношении всех сотрудников.

AWS не ведет кампанию по назначению протокола TLS 1.0 устаревшим для всех сервисов, так как некоторым клиентам (не подпадающим под требования PCI) данный протокол требуется. Однако сервисы AWS оценивают воздействие отключения TLS 1.0 на клиентов в индивидуальном порядке и в некоторых случаях могут назначить этот протокол устаревшим. Также клиенты могут использовать конечные точки FIPS, чтобы использовать надежную криптографию. AWS будет обновлять все конечные точки FIPS минимум до версии TLS 1.2. Подробные сведения приведены в этой публикации в блоге.

Все сервисы AWS, соответствующие требованиям PCI, поддерживают TLS 1.1 или более новых версий. Некоторые из этих сервисов также поддерживают TLS 1.0 для клиентов (не подпадающих под требования PCI), которым нужен данный протокол. Клиенты должны самостоятельно обновить свои системы, чтобы обеспечить взаимодействие с сервисами AWS, использующими защищенный протокол TLS, например TLS 1.1 или выше. От клиентов требуется использовать и настроить балансировщики нагрузки AWS (Application Load Balancer или Classic Load Balancer) для защищенного обмена данными по протоколу TLS 1.1 или более новой версии. Для этого им нужно выбрать предопределенную политику безопасности AWS, способную обеспечить обмен данными с применением протокола шифрования между клиентом и балансировщиком нагрузки, например TLS 1.2. К примеру, политика безопасности балансировщика нагрузки AWS ELBSecurityPolicy-TLS-1-2-2018-06 поддерживает только TLS 1.2.

Если сканирование, выполненное утвержденным поставщиком услуг сканирования (ASV) клиента, выявит наличие TLS 1.0 в конечной точке API AWS, это значит, что API все еще поддерживает TLS 1.0, а также TLS 1.1 и более поздние версии. Некоторые сервисы AWS, соответствующие требованиям PCI, по-прежнему поддерживают TLS 1.0 для клиентов, которым необходим этот протокол для рабочих нагрузок вне сферы PCI. Клиенты могут доказать ASV, что конечная точка API AWS поддерживает TLS 1.1 и более новых версий с помощью инструмента, например Qualys SSL Labs, для определения используемого протокола. Клиенты могут также доказать, что они используют защищенный обмен данными по протоколу TLS, при подключении с помощью балансировщика нагрузки AWS Elastic Load Balancer, который настроен с помощью соответствующей политики безопасности балансировщиков нагрузки AWS, поддерживающей TLS 1.1 или выше (например, ELBSecurityPolicy-TLS-1-2-2017-01 поддерживает только v1.2). ASV может потребовать от клиента пройти через процесс спора о наличии уязвимости, и представленные доказательства могут выступить в качестве подтверждения соответствия требованиям. Раннее обращение в ASV и предоставление ему доказательств перед выполнением сканирования также может упростить процесс оценки и поможет успешно пройти сканирование.

Ресурсы по PCI DSS

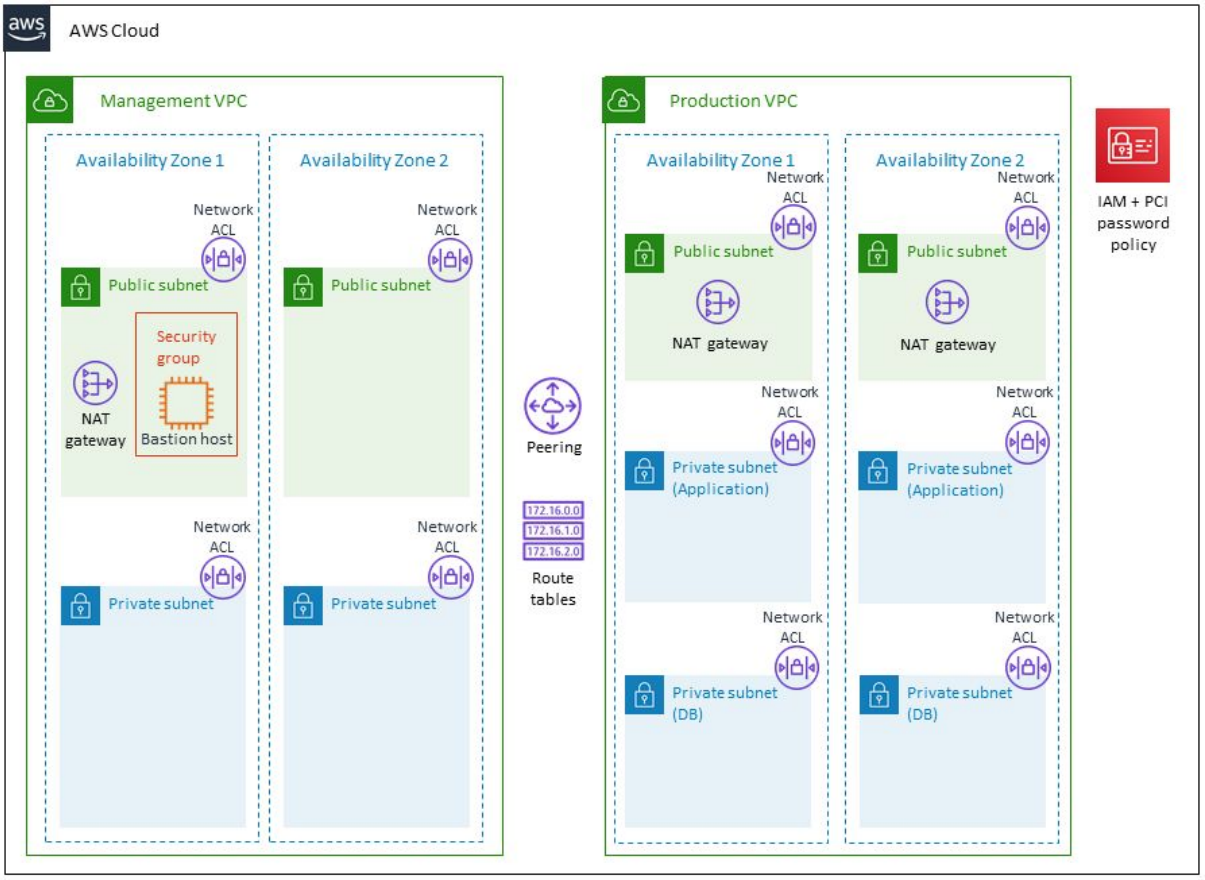
- Руководство по обеспечению соответствия требованиям: PCI DSS 3.2.1 на AWS
- Техническое описание AWS PCI 3DS
- Краткое руководство: соответствие требованиям PCI DSS в AWS
- Рекомендации по виртуализации PCI DSS
- Рекомендации PCI DSS по облачным вычислениям
- Обзор средств защиты Amazon GuardDuty: соответствие требованиям PCI DSS

Пример инфраструктуры в AWS QuickStart в соответствии с требованиями PCI DSS

В AWS QuickStart представлен готовый пакет шаблонов AWS CloudFormation для автоматического развертывания инфраструктуры в соответствии с требованиями PCI DSS version 3.2.1.
Данный пакет шаблонов Quick Start позволит автоматически настроить соответствующие ресурсы AWS и развернуть многоуровневое веб-приложение на базе Linux. Пакет включает в себя основной шаблон для начальной настройки и три дополнительных шаблона для дополнительной настройки. Краткое руководство содержит справочник по элементам управления безопасностью, в котором показано соответствие компонентов конфигурации, рассматриваемого пакета Quick Start требованиям PCI DSS. Этот пакет Quick Start является частью того, что AWS предлагает по обеспечению соответствия инфраструктуры приложений нормативным требованиям, чтобы помочь поставщикам услуг аутсорсинга (MSPs), разработчикам, интеграторам и компаниям по информационной безопасности соблюдать строгие требования к безопасности и управлению рисками.
Рассматриваемый пакет шаблонов состоит из основного и трех дополнительных. Используя основной можно развернуть облачную инфраструктуру в соответствии с требованиями PCI DSS. Он состоит из:

- Базовой конфигурации AWS Identity and Access Management (IAM), в которой представлены IAM политики, группы, роли, и профили инстансов.
- PCI-совместимых политик паролей.
- Виртуального частного (приватного) облака (VPC) с архитектурой в нескольких зонах доступности с отдельными подсетями для разных уровней приложений и приватными подсетями (не имеющими прямой маршрутизации в интернет) для приложения и базы данных.
- NAT gateways предоставляющего доступ в интернет для ресурсов, находящихся в приватных подсетях.
- Защищенного хоста (bastion host) для подключения по Secure Shell (SSH) к инстансам (Amazon EC2) с целью администрирования и решения различного рода проблем.
- Network access control list (network ACL) для фильтрации трафика.
- Standard security groups для EC2 инстансов.

Схема для основного пакета шаблонов



Дополнительные пакеты шаблонов предоставляют следующие возможности:

A. Разворачивание системы логирования, мониторинга и оповещения с использованием AWS CloudTrail, AWS CloudWatch. А также, при необходимости, централизованное управление конфигурациями ресурсов на основе AWS Config.
B. Поднятие кластера базы данных на основе Amazon RDS .

C. Инсталляция трехуровневой архитектуры Web приложения на основе операционной системы Linux с Autoscaling, Application Load Balancer и AWS WAF.

Схема для пакета шаблонов A

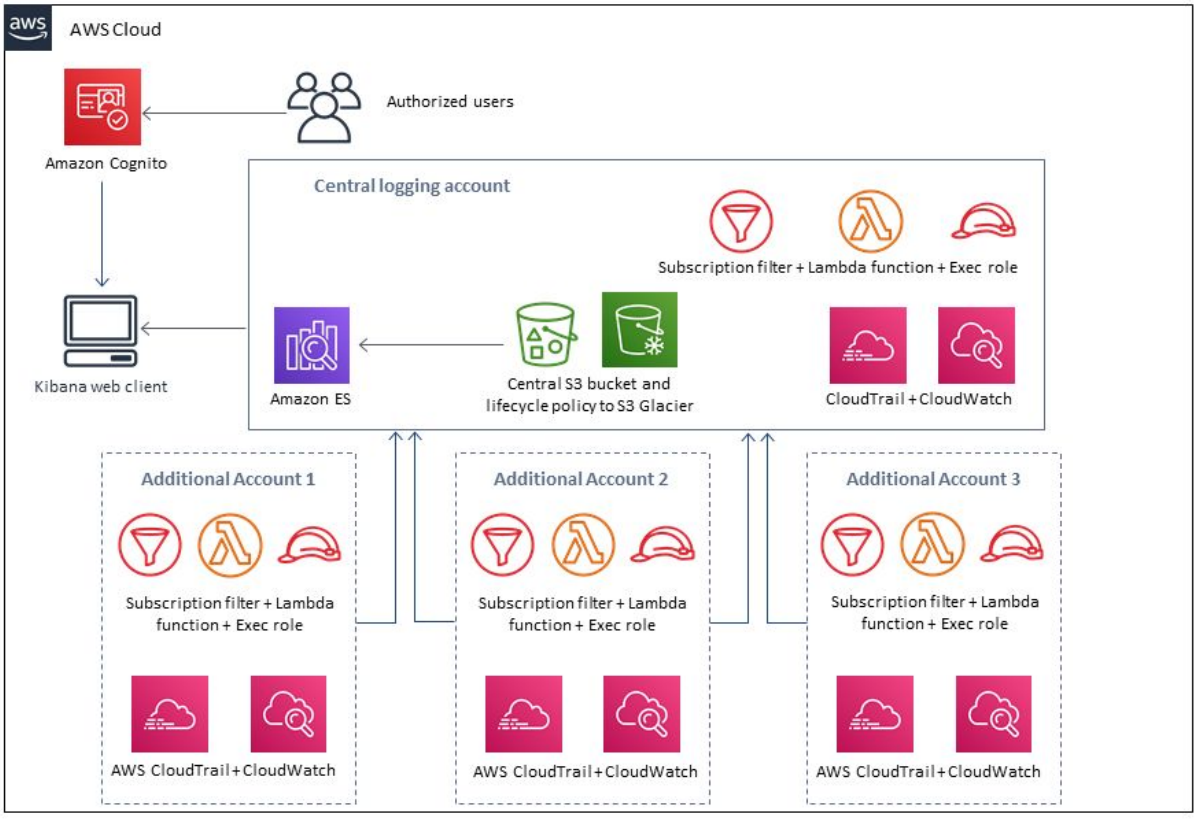


Схема для пакета шаблонов B

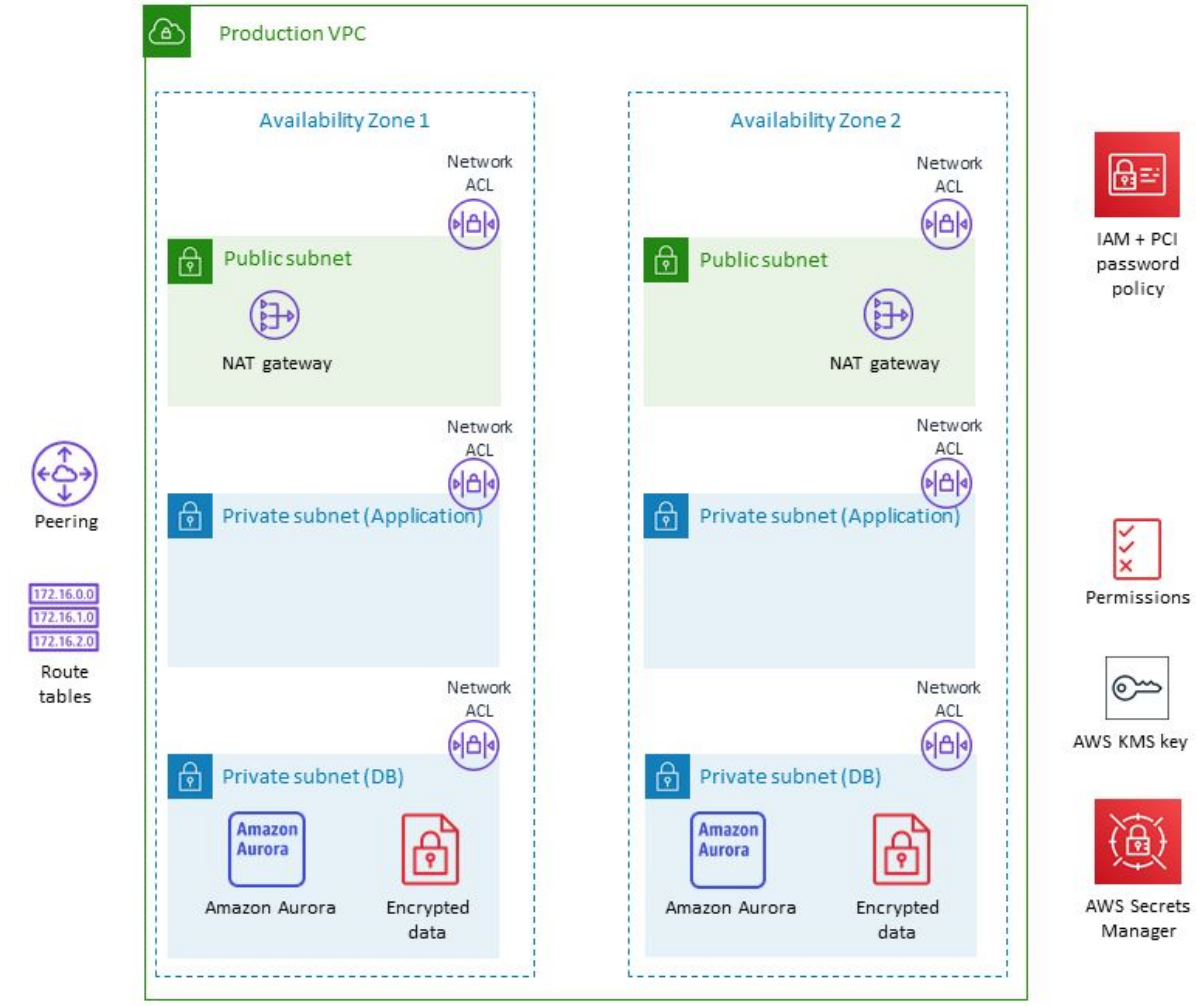


Схема для пакета шаблонов C