AWS Microsoft Workloads Competency

Контрольный список проверки технологического партнера

Июнь 2019 г.

Версия 1.0

aws partner network

Содержание

Содержание....2
Введение....3
Ожидания сторон....3
Программа AWS Microsoft Workloads Competency....4
Категории AWS Microsoft Workloads Competency....4
Требования программы AWS Microsoft Workloads Competency....5
Контрольный список для программы AWS Microsoft Workloads Competency....8
Технические требования к рабочим нагрузкам Microsoft по категориям....8
Миграция рабочих нагрузок Microsoft....8
оптимизация операций.....9
Данные, аналитика и машинное обучение....10
Технические требования AWS....12

Введение

Задача программы AWS Competency заключается в выявлении партнеров партнерской сети AWS («Партнеры APN»), которые подтвердили свой технический профессионализм и успешную работу с клиентами в сфере специализированных решений. Контрольный список проверки партнера в рамках программы AWS Competency («Контрольный список») предназначен для партнеров APN, которые хотят подать заявку на участие в программе AWS Competency. В контрольном списке приведены критерии для получения соответствующего статуса в программе AWS Competency. После подачи заявки по конкретной специализации программы Competency партнерам APN необходимо пройти аудит. Для проведения аудита AWS привлекает как собственных экспертов, так и сторонние компании. AWS оставляет за собой право вносить изменения в настоящий документ в любое время.

Ожидания сторон

Предполагается, что партнеры APN даже при соответствии всем требованиям внимательно изучат настоящий документ перед подачей заявки на участие в программе AWS Competency. Если содержимое настоящего документа неясно и требуется дальнейшее пояснение, свяжитесь сначала с представителем AWS по развитию партнеров (PDR) или менеджером AWS по развитию партнеров (PDM). При необходимости дальнейшей помощи ваш PDR или PDM обратится в офис программы.

Когда заявка будет готова к подаче, партнеры APN должны заполнить колонку самооценки в контрольном списке, который приведен в продолжении настоящего документа.

Для отправки заявки выполните следующие действия.

1. Авторизуйтесь на портале партнеров APN (https://partnercentral.awspartner.com/) в качестве главного специалиста Alliance.
2. Выберите «View My APN Account» в левой части страницы.
3. Перейдите к разделу «Program Details».
4. Выберите «Update» рядом с программой AWS Competency, на которую подается заявка.
5. Заполните заявку и нажмите «Submit».
6. Отправьте заполненную самооценку по адресу competency-checklist@amazon.com.
    - Самооценка должна включать следующее:
        - Категория решения (разработка продукта, разработка рабочей среды, рабочая среда или операции)
        - Тип развертывания (SaaS-решение или решение с самостоятельным развертыванием на AWS)
        - Документацию для примеров использования AWS (см. определения ниже)

Если у вас есть вопросы по этим инструкциям, обратитесь к своему представителю по развитию партнеров (PDR) или менеджеру по развитию партнеров (PDM).

AWS рассмотрит заявку и ответит в течение пяти рабочих дней, чтобы начать подготовку к планированию аудита или запросить дополнительную информацию.

Партнеры APN должны подготовиться к аудиту: прочитать контрольный список, выполнить самооценку с помощью контрольного списка, а также собрать и систематизировать фактические данные, чтобы предоставить их аудитору в назначенное время аудита.

AWS рекомендует, чтобы партнеры APN выделили на время аудита сотрудников, обладающих глубокими знаниями по требованиям аудита. Партнеру APN рекомендуется обеспечить доступность следующих сотрудников в ходе аудита: одного или несколько инженеров или архитекторов с большим техническим опытом, прошедших обучение и получивших сертификаты AWS; операционного менеджера, который отвечает за операции и поддержку; менеджера по развитию бизнеса для проведения обзорного доклада. До назначения даты аудита партнеры APN должны дать согласие на предоставление аудитору (AWS или другой стороне) всей информации, представленной в виде объективных данных или демонстраций.

Программа AWS Microsoft Workloads Competency

В рамках настоящей программы AWS Microsoft Workloads Competency (далее – «AWS Microsoft Workloads Competency» или «Competency») проводится выявление и проверка решений технологических партнеров APN, способных помочь клиентам в оценке и миграции рабочих нагрузок Microsoft в AWS, а также в развертывании, оптимизации и модернизации рабочих нагрузок Microsoft в AWS. Подходящие предложения распределяются по трем категориям: «Миграция», «Оптимизация операций» и «Данные / аналитика / машинное обучение». Эти категории, в свою очередь, делятся на функциональные подкатегории. Партнеры APN могут подать заявку и стать участниками программы AWS Competency в одной или нескольких категориях.

Категории AWS Microsoft Workloads Competency

Партнеру APN необходимо определить категорию и подкатегорию (или несколько категорий) сегмента для своего решения.

1. **Миграция рабочих нагрузок Microsoft.** Технологии этой категории позволяют выполнять предварительную оценку, планирование или автоматизацию процесса миграции рабочих нагрузок Microsoft и управлять этим процессом.
2. **Оптимизация операций.** Технологии этой категории используются для оптимизации и автоматизации рабочих нагрузок Microsoft в AWS в таких областях, как безопасность, доступность и управляемость.
3. **Данные, анализ и машинное обучение.** Технологии этой категории помогают выполнять подготовку, преобразование, анализ данных Microsoft SQL Server, а также управление ими для дальнейшего анализа данных и машинного обучения на AWS.

Таблица была изменена

Требования программы AWS Microsoft Workloads Competency

Ниже приведены параметры, которые будут оцениваться менеджером программы AWS Competency. Прежде чем назначать время технологической проверки, необходимо собрать всю недостающую информацию.

1.0. Требования программы APN		**Соответствие: да / нет**
1.1. Руководство по программе	Перед подачей заявки на участие в программе Microsoft Workloads Competency партнеру APN необходимо прочитать руководство по программе и соответствующие определения. Нажмите здесь, чтобы просмотреть подробные сведения о программе.	
1.2. Уровень технологического партнера APN	Партнер APN должен являться опытным технологическим партнером APN.	
1.3. Категория решения	Партнер APN должен определить свое решение в определенную категорию или подкатегорию (несколько подкатегорий) сегмента. Категория ▪ **Миграция рабочих нагрузок Microsoft** ☐ Оценка перед миграцией ☐ Миграция приложений и данных ☐ Состояние миграции ☐ Мониторинг и отчетность ▪ **Оптимизация операций рабочих нагрузок Microsoft** ☐ Управление безопасностью и угрозами ☐ Доступность и аварийное восстановление ☐ Управление ресурсами, мониторинг и отчетность по запасам / состоянию / расходам Управление ресурсами, мониторинг и отчетность по запасам / состоянию / расходам ▪ **Данные, аналитика и машинное обучение для рабочих нагрузок Microsoft** ☐ Интеграция и подготовка данных ☐ Решения для платформ ☐ Решения для SaaS и API ☐ Бизнес-аналитика и визуализация ☐ Управление данными, обеспечение соответствия требованиям и безопасность	
2.0. Примеры использования		**Соответствие: да / нет**
2.1. Рабочие нагрузки Microsoft: конкретные примеры использования	Партнер APN должен представить не менее 4 (четырех) примеров использования, которые демонстрируют применение технологии партнера APN, относящейся к рассматриваемой категории. Для партнеров APN, уже получивших в рамках программы AWS Competency соответствующий статус по специализациям «Миграция», DevOps или «Данные и аналитика», это требование сокращено до двух примеров использования (одного общедоступного и одного частного), демонстрирующих применение технологии партнера APN, относящейся к рассматриваемой категории, с рабочими нагрузками Microsoft. Если рассматривается несколько категорий, требуется не менее одного примера использования технологии в каждой подкатегории. Для каждого примера использования партнер APN должен предоставить следующую информацию. ▪ Имя клиента ▪ Проблема клиента	

	▪ Каким образом было выполнено развертывание решения для устранения проблемы ▪ Использованные приложения или решения сторонних разработчиков ▪ Дата начала эксплуатации ▪ Итоги / результаты ▪ Конкретные схемы архитектур, руководства по развертыванию и другие материалы в зависимости от типа решения, как описано в следующем разделе Эта информация будет запрошена в рамках процесса подачи заявки на участие в программе на портале партнеров APN. Все четыре представленных примера использования будут оцениваться в ходе технической проверки. Если партнер APN не сможет представить документацию, необходимую для оценки примера использования по каждому пункту контрольного списка, или какие-либо требования контрольного списка не будут удовлетворены, пример использования будет снят с рассмотрения на участие в программе AWS Competency. Примеры использования должны содержать описания развертываний, выполненных в течение последних 18 месяцев. Кроме того, они должны представлять собой рабочие проекты, используемые клиентами, а не «пилотные» проекты или опытные образцы.	
2.2. Общедоступные примеры использования	Общедоступные примеры использования применяются AWS после принятия партнера APN в программу Competency для того, чтобы продемонстрировать успех его решения с помощью измеримых ключевых показателей эффективности (KPI) и убедить клиентов в том, что партнер APN обладает технологиями, отвечающих поставленным целям. По конкретным примерам использования партнер APN должен представить 2 (два) из 4 (четырех) развертываний у клиентов в качестве общедоступных примеров использования. Эти общедоступные примеры использования могут представлять собой формальные примеры использования, технические документы, видеоматериалы или публикации в блогах.	
	Примеры использования для общего ознакомления должны быть доступны на веб-сайте партнера APN, т. е. должна существовать возможность перехода к общедоступным примерам использования с главной страницы партнера APN. Партнер APN должен предоставить ссылки на эти общедоступные примеры использования в своей заявке.	
	Общедоступные примеры использования должны содержать следующую информацию. ▪ Имя клиента, имя партнера APN и AWS ▪ Проблема клиента ▪ Каким образом было выполнено развертывание решения для устранения проблемы ▪ Каким образом сервисы AWS использовались при создании решения ▪ Итоги / результаты	
3.0. Присутствие в Интернете и экспертное позиционирование участника программы AWS Microsoft Workloads		**Соответствие: да / нет**
3.1. Микросайт партнера AWS	Присутствие партнера APN в Интернете, связанное с его решениями в рамках программы AWS Microsoft Workloads, является для клиентов подтверждением его возможностей и опыта. У партнера APN должен быть микросайт AWS, содержащий описание его решения для участия в программе AWS Microsoft Workloads, ссылки на общедоступные примеры использования, список партнеров-технологов и любую другую значимую информацию, которая демонстрирует опыт партнера в использовании рабочих нагрузок Microsoft и подчеркивает его партнерство с AWS. Этот микросайт, посвященный рабочим нагрузкам Microsoft на AWS, должен быть доступен с главной страницы партнера APN. Использовать саму домашнюю страницу в качестве микросайта AWS нельзя. Исключение представляет собой ситуация, когда партнер APN – компания, специализирующаяся на рабочих нагрузках Microsoft, и домашняя страница это отражает.	

3.2. Экспертное позиционирование участника программы Microsoft Workloads	Предполагается, что партнеры программы AWS Microsoft Workloads Competency обладают экспертными знаниями в области управления облаком и разработали инновационные решения, которые включают в себя сервисы AWS или помогают ими управлять. Партнеры APN должны предоставить публичные материалы (например, публикации в блогах, печатные статьи, видеоролики и т. д.), демонстрирующие внимание партнера APN к рабочим нагрузкам Microsoft и опыт их использования. Необходимо предоставить ссылки на примеры материалов, опубликованных в течение последних 12 месяцев.	
4.0. Требования к бизнесу		**Соответствие: да / нет**
4.1. Поддержка продукта / служба технической поддержки	Партнер APN осуществляет поддержку клиентов через веб-чат, телефон или электронную почту. Необходимо подтверждение этого факта в виде описания поддержки, доступной клиентам по их продуктам или решениям.	
4.2. Размещение продукта в AWS Marketplace	Партнер APN предоставляет решение через AWS Marketplace. ☐ Да ☐ Нет Если да, партнер APN должен предоставить ссылку на AWS Marketplace. Если нет, дополнительной информации не требуется. Примечание. Для получения статуса в программе Competency размещение в AWS Marketplace не является обязательным.	
4.3. Модель развертывания	Партнер APN определяет все доступные клиентам варианты модели развертывания. ☐ SaaS на AWS ☐ SaaS вне AWS (для миграции) ☐ BYOL на AWS ☐ BYOL локально (для миграции)	
5.0. Самооценка партнера APN		**Соответствие: да / нет**
5.1. Контрольный список самооценки для партнерской программы AWS Competency	Партнер APN должен провести самооценку своего соответствия данному контрольному списку. ▪ Партнер APN должен заполнить все разделы контрольного списка. ▪ Заполненную самооценку необходимо отправить по адресу **competency-checklist@amazon.com**. Поле темы необходимо заполнить следующим образом: «[Имя партнера APN], Microsoft Workloads Competency Technology Partner Completed Self-Assessment». ▪ Перед отправкой заполненной самооценки в AWS партнеру APN рекомендуется передать заявку на проверку своему архитектору партнерских решений, PDR или PDM. Такая рекомендация объясняется тем, что команда AWS партнера APN должна участвовать в процессе и предоставлять рекомендации еще до проверки. Кроме того, это повышает эффективность процедуры проверки.	

Контрольный список для программы AWS Microsoft Workloads Competency

Следующие пункты будут проверяться архитектором партнерских решений AWS и (или) сторонними аудиторами и (или) архитекторами партнерских решений AWS. Недостающую информацию следует предоставить до планирования технической проверки.

Технические требования к рабочим нагрузкам Microsoft по категориям

В рамках самооценки для программы AWS Competency необходимо предоставить документацию, в которой описано, как решение партнера APN удовлетворяет требованиям.

Миграция рабочих нагрузок Microsoft

Обязательные возможности решения		Соответствие: да / нет

Оценка перед миграцией	В техническом решении должна применяться технология (с использованием агента или без такового) в целях автоматического выявления рабочих нагрузок для миграции в AWS. Это может включать следующее.
	▪ Предварительную оценку перед миграцией рабочих нагрузок Microsoft для одного или нескольких перечисленных пунктов.
	  ○ Оценка локальных серверов и виртуальных машин с Microsoft Windows
	  ○ Оценка контейнеров Docker (на основе Windows Server или содержащих приложения .NET/.NET Core)
	  ○ Оценка приложения .NET/.NET Core
	  ○ Оценка данных для миграции (SQL, файловая система, BLOB-объекты и пр.)
	  ○ Оценка возможностей миграции корпоративных решений (Active Directory, OneDrive, Dynamics, Exchange и пр.)
	▪ По результатам предварительной оценки перед миграцией необходимо составить отчет.
	в группу ресурсов AWS, указанную клиентом для каждой рабочей нагрузки	

Миграция	В техническом решении должна применяться технология (с использованием агента или без такового) для автоматической миграции выявленных рабочих нагрузок на AWS или миграции данных в составе рабочих нагрузок. Это может включать следующее.
	▪ Миграция рабочих нагрузок Microsoft для одного или нескольких перечисленных пунктов.
	  ○ Миграция виртуальных машин
	  ○ Миграция контейнеров Docker (на основе Windows Server или содержащих приложения .NET/.NET Core)
	  ○ Миграция приложения .NET/.NET Core
	  ○ Миграция данных (SQL, файловая система, BLOB-объекты и пр.)
	  ○ Миграция корпоративных решений (Active Directory, OneDrive, Dynamics, Exchange и пр.)
	▪ Возможность выполнять резервное копирование и откат в случае неудачи какого-либо этапа миграции в любой момент времени без потери данных (или с минимальной потерей)
	▪ Использование гибридных облачных конфигураций для аварийного восстановления
	▪ Дифференциальная синхронизация изменений с целью синхронизации данных после миграции до отключения и прекращения работы исходного сервера или инстанса
	▪ Прямая миграция отдельной рабочей нагрузки в группу ресурсов AWS, указанную клиентом	

Состояние миграции	Техническое решение во время миграции должно выполнять оценку в реальном времени по перечисленным параметрам: ▪ целостность данных; ▪ работоспособность приложений; ▪ общую оценку работоспособности связной архитектуры;	
мониторинг и отчетность;	Техническое решение должно иметь следующие возможности. ▪ Мониторинг процесса миграции ▪ Уведомления, предупреждения и ведение отчетности об ошибках ▪ предоставление общего отчета о миграции;	

оптимизация операций.

Обязательные возможности решения		**Соответствие: да / нет**
Безопасность	Техническое решение должно выполнять следующие задачи. ▪ Конфигурация мер безопасности (доступ на основании ролей, управление идентификацией и доступом, конфигурация прокси-сервера или брандмауэра, маршрутизация, шифрование и пр.) ▪ Анализ в целях защиты от потери данных (DLP) ▪ Обеспечение мер сетевой безопасности и безопасности инстанса (порты, сертификаты, настройка безопасности) ▪ Моделирование угроз для сетевого трафика (возможных векторов атаки) и предупреждение ▪ Обеспечение соответствия требованиям (HIPAA, PCI, SOX и пр.) ▪ Возможность рекомендовать усиление мер безопасности ▪ Проверка исходного кода на предмет неудачных методов, утечек памяти, санации данных и проблем безопасности	

Обеспечение доступности	Техническое решение должно выполнять следующие задачи.
	▪ Непрерывная проверка возможностей аварийного восстановления (хаос-инжиниринг)
	  ○ Обеспечение масштабируемости
	  ○ Обеспечение доступности
	  ○ Обеспечение целостности и устойчивости данных
	▪ Анализ ресурсов для выявления проблем с высокой доступностью.
	▪ Способность автоматического масштабирования (в сторону уменьшения и увеличения) по мере изменения рабочей нагрузки	

Управление	Техническое решение должно выполнять следующие задачи.
	▪ Инвентаризация и анализ (в инстансах Amazon EC2, контейнерах, бессерверной архитектуре):
	  ○ ресурсов рабочих нагрузок Microsoft;
	  ○ конфигурации рабочих нагрузок Microsoft;
	  ○ конфигурации инфраструктуры Microsoft.
	▪ Автоматическое обнаружение:
	  ○ Конфигурация сети
	  ○ Вычислительные ресурсы (серверы, кластеры)
	  ○ Ресурсы хранилища (логические номера устройств, конечные объекты iSCSI и пр.)	

	○ Базы данных (ядра, конфигурация, версия, совместимость) ▪ Ретроспективный анализ изменений в инвентаризации (за выбранный период) ▪ Анализ выделения ресурсов и уровня использования ▪ Непрерывный анализ затрат и предупреждение (использование и лицензирование ресурсов) ▪ Возможность рекомендовать ограниченное предоставление ресурсов на основе шаблонов рабочей нагрузки и использования ▪ Непрерывный анализ производительности и предупреждение ▪ Общие оперативные задачи автоматизации, характерные для рабочих нагрузок Microsoft, примеры которых перечислены ниже. ○ Резервное копирование и восстановление ○ Исправление ○ Управление состоянием рабочих нагрузок ○ Управление конфигурацией ▪ Эталонное тестирование требуемой или средней производительности локальных решений или приложений ▪ Подбор инстансов, ресурсов и предоставление рекомендаций по AWS на основе эталонного тестирования ▪ Тестирование опытного образца и эталонное тестирование решений или приложений на AWS ▪ Примерная оценка совокупной стоимости владения (TCO) и использования ресурсов на основе эталонного тестирования ▪ Отчетность. ○ Отчетность о производительности, доставка и предупреждения (для отчетов) ○ Отчетность об инфраструктуре, доставка и предупреждения (для отчетов) ○ Отчетность о конфигурации рабочих нагрузок и работоспособности, доставка и предупреждения (для отчетов) ○ Отчетность об исправлениях, доставка и предупреждения (для отчетов)	

Данные, аналитика и машинное обучение

Обязательные возможности решения		Соответствие: да / нет
Интеграция и подготовка данных	Техническое решение должно иметь следующие возможности. ▪ Прием данных рабочих нагрузок и предложение действий ▪ Добавление примечаний к описательным, структурным, административным, справочным и статистическим данным: ○ группировка синтаксических деревьев и деревьев зависимостей, в том числе выявление кореференции; ○ семантическое аннотирование текста, в том числе выявление именованных сущностей для приложений поиска, анализа настроений и интеллектуального анализа данных; ○ определение языка, диалекта и демографических данных говорящего; ○ видео, изображения, файлы в формате Word, PDF и т. д.;	

	○ отдел, филиал, процесс; ○ уровень обеспечения безопасности (конфиденциальный, общедоступный, частный и т. д.); ○ тип объекта (здание, человек, животное и т. д.). ▪ Перемещение и объединение данных из разрозненных источников ▪ Преобразование и подготовка данных к аналитике ▪ Проверка качества данных ▪ Репликация данных ▪ Профилирование данных ▪ Проектирование возможностей – создание новых возможностей из уже существующих	
Решения для платформ	Техническое решение должно обладать следующими характеристиками. ▪ Представлять собой тесно связанные инструменты, предназначенные для совместной работы и решения проблем аналитики в рамках стандартизированной платформы. Может содержать следующие компоненты: ○ хранилище; ○ обработка; ○ планирование; ○ безопасность; ○ аналитические объекты. ▪ Предоставлять специалистам по работе с данными и специалистам по машинному обучению инструменты для выбора данных, обучения прогнозных моделей и создания прогнозов на основе новых данных.	
Решения для SaaS и API	В эту категорию входят решения, обеспечивающие прогнозные возможности в приложениях клиентов (с использованием искусственного интеллекта и машинного обучения). ▪ Веб ▪ Клиент ▪ Платформы	
Бизнес-аналитика и визуализация	Технические решения, которые преобразуют необработанные данные в рабочие бизнес-данные с помощью аналитических информационных технологий. К ним относятся: ▪ ведение отчетности; ▪ панели управления; ▪ визуализация данных.	
Управление данными и обеспечение их безопасности	Технические решения для обнаружения, упорядочивания данных и управления ими. Сюда относятся следующие возможности. ▪ Определение и осуществление политик ▪ Обеспечение безопасности персональных данных и управление ими ▪ Создание каталогов данных и глоссариев ▪ Определение происхождения данных ▪ Маскирование данных	

Технические требования AWS

Ниже приведены технические требования к каждому из четырех примеров использования, предоставленных партнером APN. Каждый из них должен демонстрировать, что решения, развертывание которых выполнено партнером APN, соответствуют рекомендациям AWS и концепции AWS Well-Architected Framework.

		Область действия				
		Многопользовательское SaaS-решение	Однопользовательское SaaS-решение	Решение клиента с локальным развертыванием	Решение клиента с развертыванием на AWS	**Соответствие: да / нет**
Необходимая документация В рамках самооценки для участия в программе Competency необходимо отправить следующую документацию.						
Схема архитектуры	В зависимости от категории развертывания требуется одна или несколько схем архитектуры. На каждой схеме архитектуры должно быть показано следующее. ▪ Основные элементы архитектуры, а также то, как они сочетаются для предоставления решения партнера APN клиентам ▪ Все задействованные сервисы AWS (с использованием соответствующих значков сервисов AWS) ▪ Способ развертывания сервисов AWS, включая информацию об Amazon Private Virtual Cloud (Amazon VPC), зонах доступности, подсетях и подключениях к системам за пределами AWS. ▪ Включаются элементы, развертывание которых выполнено за пределами AWS, например локальные компоненты или аппаратные устройства.	Да – для всего решения и для каждого примера использования	Да – для всего решения и для каждого примера использования	Да – для каждого примера использования	Да – для каждого примера использования	
Руководство по развертыванию	Руководство по развертыванию должно содержать рекомендации по развертыванию решения партнера APN на AWS и включать все разделы, перечисленные в документе Baseline Requirements for Deployment Guides.	Нет	Нет	Нет	Да – одно для решения	
Заполненный контрольный список проверки	Для каждого из четырех примеров использования партнеру APN необходимо предоставить заполненный контрольный список, образец которого приведен ниже.	Да	Да	Да	Да	
1.0. Безопасность Основополагающие элементы безопасности – защита информации и систем. К основным аспектам относятся конфиденциальность и целостность данных, определение возможностей пользователей и управление ими посредством привилегий, защита систем, а также установка элементов управления для обнаружения событий безопасности.						
1.1. Пользователь root учетной записи AWS не используется для стандартных действий	Пользователя root учетной записи AWS запрещено использовать для выполнения стандартных действий. Сразу после создания учетной записи AWS необходимо создать учетные записи пользователей AWS Identity and Access Management (IAM), а затем использовать их для выполнения всех стандартных действий. После создания учетных записей	Да	Да	Нет	Нет	

	пользователей IAM необходимо в надежном месте сохранить учетные данные пользователя root и использовать их только для выполнения некоторых задач, связанных с управлением учетными записями и сервисами AWS, которые этого требуют. Подробнее о том, как настраивать учетные записи и группы пользователей IAM для ежедневного использования, см. в разделе Creating Your First IAM Admin User and Group.					
1.2. Для пользователя root учетной записи AWS включена возможность Multi-Factor Authentication (MFA)	Для пользователя root учетной записи AWS необходимо включить возможность Multi-Factor Authentication (MFA). Поскольку пользователь root учетной записи AWS может выполнять конфиденциальные операции, дополнительный уровень аутентификации позволит надежнее защитить учетную запись. Доступно несколько типов MFA, в том числе виртуальная MFA и аппаратная MFA.	Да	Да	Нет	Нет	
1.3. Для всех стандартных действий используются учетные записи пользователей IAM	Запрещается использовать пользователя root учетной записи AWS для выполнения задач, которые этого не требуют. Вместо этого создайте новых пользователей IAM для всех лиц, которым требуется доступ от имени администратора. Затем сделайте этих пользователей администраторами. Для этого поместите их в группу администраторов, к которой необходимо прикрепить управляемую политику AdministratorAccess. Пользователи, находящиеся в группе администраторов, должны настраивать группы, пользователей и т. д. для аккаунта AWS. Все последующие взаимодействия необходимо осуществлять через пользователей учетной записи AWS и их собственные ключи, а не через пользователя root. Однако для выполнения некоторых задач по управлению учетной записью и сервисами необходимо входить в систему с использованием учетных данных пользователя root.	Да	Да	Нет	Нет	
1.4. Для всех интерактивных пользователей IAM включена возможность Multi-Factor Authentication (MFA)	Необходимо включить возможность Multi-Factor Authentication (MFA) для всех интерактивных пользователей IAM. Когда включена возможность MFA, у пользователей есть устройство, генерирующее уникальный код аутентификации (одноразовый пароль, или OTP). Пользователи должны предоставить как стандартные учетные данные (имя пользователя и пароль), так и OTP. В качестве устройства MFA может использоваться либо аппаратное обеспечение, либо виртуальное устройство (например, его можно запускать в приложении на смартфоне).	Да	Да	Нет	Нет	
1.5. Выполняется регулярная ротация учетных данных IAM	Необходимо регулярно менять пароли и ключи доступа, а также следить за тем, чтобы это делали и другие пользователи IAM в вашей учетной записи. Таким образом, если пароль или ключ доступа будет скомпрометирован без вашего ведома, вы ограничите время, в течение которого можно получить доступ к ресурсам с использованием этих учетных данных. К учетной записи можно применить политику паролей, которая требует ротации паролей от всех пользователей IAM. Можно также выбрать частоту, с которой они должны это делать. Подробнее о ротации ключей доступа для пользователей IAM см.	Да	Да	Да (для учетных данных, которые используются для интеграции с AWS)	Да (для учетных данных, которые используются для интеграции с AWS)	

	в разделе Rotating Access Keys.					
1.7. Для пользователей IAM действует политика надежных паролей	Для пользователей IAM необходимо настроить политику надежных паролей. Если пользователям разрешено менять пароли самостоятельно, необходимо требовать, чтобы они создавали надежные пароли и выполняли их ротацию через определенные промежутки времени. Создать политику паролей для своей учетной записи можно на странице настроек учетной записи в консоли IAM. Политику паролей можно использовать для определения требований к паролям, таких как минимальная длина, необходимость использования небуквенных символов, частота ротации и т. д. Подробнее см. в разделе Setting an Account Password Policy for IAM Users.	Да	Да	Да (для учетных данных, которые используются для интеграции с AWS)	Да (для учетных данных, которые используются для интеграции с AWS)	
1.8. Одни и те же учетные данные IAM не используются для разных пользователей	Для каждого лица, которому требуется доступ к вашей учетной записи AWS, необходимо создать отдельную учетную запись пользователя IAM. Создайте пользователя IAM также и для себя, наделите его правами администратора и выполняйте всю работу от его имени. При создании отдельных пользователей IAM для лиц, которым требуется доступ к вашей учетной записи, каждому из них можно назначить уникальный набор учетных данных для доступа. Кроме того, всем пользователям IAM можно предоставлять различные разрешения. При необходимости в любой момент можно изменить или отменить разрешения пользователя IAM. (Если вы выдаете учетные данные пользователя root, отозвать их трудно. Кроме того, невозможно ограничить разрешения.)	Да	Да	Нет	Нет	
1.9. Действие политик IAM подчиняется принципу минимальных привилегий	Необходимо следовать стандартной рекомендации по безопасности, суть которой заключается в предоставлении минимальных привилегий. Иными словами, даются только разрешения, необходимые для выполнения задачи. Определите, что должны сделать пользователи, и создайте для них политики, которые позволят им выполнить только эти задачи. Начните с минимального набора разрешений и по мере необходимости давайте дополнительные. Такой принцип работы безопаснее ситуации, когда приходится ужесточать изначально нестрогие разрешения. Чтобы задать надлежащий набор разрешений, необходимо провести небольшое исследование. Определите, что требуется для решения определенной задачи, какие действия поддерживает конкретный сервис и какие разрешения необходимы для выполнения этих действий.	Да	Да	Да (для решений, которые работают за пределами AWS и интегрируются через роли IAM, необходимо применять доступ по принципу минимальных привилегий)	Да (для решений, которые работают за пределами AWS и интегрируются через роли IAM, необходимо применять доступ по принципу минимальных привилегий)	
1.10. Учетные данные (например, ключи доступа) не прописаны в исходном коде	Необходимо следовать рекомендациям по управлению ключами доступа AWS и не прописывать учетные данные в исходном коде. При программном доступе к AWS ключ доступа используется для подтверждения личности и удостоверения приложений. Любое лицо, у которого имеется ваш ключ доступа, обладает тем же уровнем доступа к вашим ресурсам AWS, что и вы. Поэтому AWS делает	Да	Да	Да (изменение учетных данных, которые используются для интеграц	Да (изменение учетных данных, которые используются для интеграци	

	все возможное для защиты ваших ключей доступа, и, в соответствии с нашей моделью общей ответственности, вам следует поступать так же.			ии с AWS, не должно вызывать трудностей, а сами учетные данные не должны быть прописаны в исходном коде)	и с AWS, не должно вызывать трудностей, а сами учетные данные не должны быть прописаны в исходном коде)	
1.11. Все хранимые данные зашифрованы	Требуется обеспечить шифрование всех хранимых данных.	Да	Да	Да (учетные данные, хранящиеся в решении партнера, которое используется для интеграции с AWS, должны быть зашифрованы)	Да (учетные данные, хранящиеся в решении партнера, которое используется для интеграции с AWS, должны быть зашифрованы)	
1.12. Ключи доступа AWS используются только интерактивными пользователями	Использование ключей доступа AWS допускается только в следующих случаях. 1. Используются людьми для доступа к сервисам AWS и надежно хранятся на устройстве, которое находится под управлением этого человека. 2. Используется сервисом для доступа к сервисам AWS, но только в случаях, когда: a) нецелесообразно использовать роль инстанса Amazon Elastic Compute Cloud (Amazon EC2), роль задания Amazon ECS или аналогичный механизм, b) ключи доступа AWS изменяются не реже раза в неделю и c) политика IAM подчиняется жестким принципам, в результате чего: i) разрешает доступ только к конкретным методам и целям и ii) запрещает доступ к подсетям, из которых осуществляется доступ к ресурсам.	Да	Да	Нет	Нет	
1.13. Сервис AWS CloudTrail включен для всех учетных записей AWS во всех регионах	Необходимо включить сервис AWS CloudTrail для всех учетных записей AWS во всех регионах. Прозрачность действий в вашей учетной записи AWS – это принципиально важный аспект безопасности и одна из эксплуатационных рекомендаций. Сервис AWS CloudTrail можно использовать для просмотра, поиска, скачивания, архивирования, анализа действий в учетной записи в пределах инфраструктуры AWS, а также для реагирования на них. Вы можете определить, кем или чем выполнено определенное действие, какие ресурсы	Да	Да	Нет	Нет	

	использовались, когда произошло событие, а также получить другие сведения, которые помогут при анализе и реагировании на активность в учетной записи AWS.					
1.14. Журналы AWS CloudTrail хранятся в корзине Amazon S3, принадлежащей другой учетной записи AWS	Журналы AWS CloudTrail необходимо помещать в корзину, принадлежащую другой учетной записи AWS, доступ к которой строго ограничен и предоставляется только для аудита и восстановления.	Да	Да	Нет	Нет	
1.15. Для корзины Amazon S3 с журналами AWS CloudTrail включено управление версиями или возможность MFA Delete	Корзину с журналами AWS CloudTrail необходимо защитить с помощью управления версиями или возможности MFA Delete.	Да	Да	Нет	Нет	
1.16. Группы безопасности Amazon EC2 строго ограничены	Все группы безопасности Amazon EC2 должны ограничивать доступ в наибольшей возможной степени. Это подразумевает по меньшей мере следующее. 1. Внедрение групп безопасности для ограничения трафика между Интернетом и Amazon VPC. 2. Внедрение групп безопасности для ограничения трафика в пределах Amazon VPC. 3. Использование максимально возможных ограничений во всех случаях.	Да	Да	Нет	Да	
1.17. Для корзин Amazon S3 в пределах вашей учетной записи установлены надлежащие уровни доступа	Необходимо внедрить надлежащие средства управления для контроля доступа к каждой корзине Amazon S3. При использовании AWS рекомендуется предоставлять доступ к ресурсам только тем лицам, которые не могут без них обойтись (принцип минимальных привилегий).	Да	Да	Нет	Нет (за исключением случая, когда решению партнера, работающему на AWS, требуется сервис S3)	
1.18. Корзины Amazon S3 настроены надлежащим образом и не открыты для всеобщего доступа.	Корзины, которые не должны находиться в открытом доступе, необходимо настроить надлежащим образом, чтобы закрыть к ним доступ. По умолчанию все корзины Amazon S3 являются частными и доступны только тем пользователям, которым явно предоставлен доступ. В большинстве примеров использования широкий публичный доступ для чтения файлов в корзинах Amazon S3 не требуется. Рекомендуется никогда не предоставлять общий доступ. Исключение составляет ситуация, когда Amazon S3 используется для размещения публичных ресурсов (например, изображений для использования на публичном веб-сайте).	Да	Да	Нет	Нет (за исключением случая, когда решению партнера, работающему на AWS, требуется сервис S3)	
1.19. Имеется механизм мониторинга, позволяющий отслеживать,	Необходимо применять механизм мониторинга или предупреждения, позволяющий определять, когда корзины Amazon S3 становятся публичными. С этой целью можно использовать, например, сервис AWS Trusted Advisor. AWS Trusted Advisor проверяет в	Да	Да	Да	Нет (за исключением случая, когда решению	

когда корзины или объекты Amazon S3 становятся публичными	Amazon S3 корзины, для которых имеются разрешения на открытый доступ. Разрешения для корзин, предоставляющие доступ к списку абсолютно всем, могут привести к непредвиденному росту затрат, если непредусмотренные пользователи с большой частотой просматривают список объектов в корзине. Разрешения для корзин, которые предоставляют доступ на загрузку / удаление абсолютно всем, создают потенциальные уязвимости безопасности, поскольку позволяют всем добавлять, изменять или удалять объекты, находящиеся в корзине. При проверке AWS Trusted Advisor изучаются явные разрешения для корзины и связанные с ними политики корзины, которые могут переопределить разрешения.				партнера, работающему на AWS, требуется сервис S3)	
1.20. Для обнаружения изменений в инстансах и контейнерах Amazon EC2 применяется механизм мониторинга	Любые изменения в используемых инстансах или контейнерах Amazon EC2 могут свидетельствовать о несанкционированной деятельности. Их необходимо как минимум записывать в журналы, находящиеся в надежном месте, чтобы впоследствии можно было провести расследование. Механизм, применяемый для этой цели, должен по крайней мере: 1) обнаруживать все изменения в ОС или файлах приложений в инстансах или контейнерах Amazon EC2, используемых в решении; 2) хранить данные об этих изменениях в надежном месте, находящемся за пределами инстанса или контейнера Amazon EC2. К примерам подходящих механизмов относятся: a) развертывание проверки целостности файлов через плановое управление конфигурацией (например, Chef, Puppet и т. д.) или специализированный инструмент (например, OSSEC, Tripwire или аналогичный инструмент); или b) расширение инструментов для управления конфигурацией с целью проверки конфигурации хоста Amazon EC2 и отправки уведомлений об обновлениях в конфигурационных файлах ключей или пакетах с использованием событий Canary (зарегистрированных инструкций no-op), настроенных таким образом, чтобы при выполнении обеспечить работоспособность сервиса на всех хостах в области видимости; или c) развертывание системы обнаружения вторжения на хост, например решения с открытым исходным кодом, такого как OSSEC с ElasticSearch и Kibana, или решения партнера. Обратите внимание, что следующий механизм не отвечает этому требованию: a) часто осуществляемые циклические изменения в инстансах или контейнерах Amazon EC2.	Да	Да	Нет	Нет	
1.21. Все данные классифицированы по уровню конфиденциальности	Все данные клиентов, обработанные и хранящиеся в рабочей нагрузке, рассматриваются и классифицируются с целью определить уровень их конфиденциальности и методы, подходящие для работы с ними.	Да	Да	Нет	Нет	
1.22. Все конфиденциальные данные зашифрованы	Все данные клиентов, классифицированные как конфиденциальные, зашифровываются при передаче и хранении.	Да	Да	Нет	Нет	
1.23. Все криптографическ	Все криптографические ключи зашифровываются при хранении и передаче, а доступ к ним для	Да	Да	Да	Да	

ие ключи находятся под надежным управлением	использования контролируется с помощью решения AWS, такого как KMS, или решения партнера APN, такого как HashiCorp Vault.					
1.24. Все передаваемые данные зашифрованы	Все данные, передаваемые в пределах VPC, зашифрованы.	Да	Да	Да	Да	
1.25. Процедура реагирования на инциденты, связанные с компьютерной безопасностью, определена и отработана	Должна быть определена процедура реагирования на инциденты, связанные с компьютерной безопасностью, для управления такими инцидентами, как несанкционированный доступ к учетной записи AWS. Эту процедуру необходимо протестировать путем внедрения мер отработки процедуры реагирования на инциденты, например провести игровой день информационной безопасности. Репетиция должна быть проведена в течение последних 12 месяцев. Это необходимо для того, чтобы подтвердить следующее: a) у соответствующих лиц имеется доступ к рабочей среде; b) соответствующие инструменты доступны; c) соответствующие лица знают, как реагировать на различные инциденты компьютерной безопасности, перечисленные в плане.	Да	Да	Нет	Нет	
2.0. Надежность Основополагающий элемент надежности – способность предотвращать сбои и быстро восстанавливаться после них для удовлетворения спроса со стороны бизнеса и клиентов. К основным аспектам относятся базовые элементы, связанные с настройкой, межпроектные требования, планирование восстановления и работа с изменениями.						
2.1. Имеется высокодоступное сетевое подключение	Сетевое подключение к решению должно быть высокодоступным. При использовании VPN или AWS Direct Connect для подключения к сетям клиентов решение должно поддерживать резервные соединения, даже если клиенты внедряют их не всегда.	Да	Да	Да	Да	
2.2. Механизмы масштабирования инфраструктуры соответствуют бизнес-требованиям	Механизмы масштабирования инфраструктуры должны соответствовать бизнес-требованиям, что достигается одним из следующих способов. 1. Внедрение механизмов автомасштабирования на каждом уровне архитектуры. 2. Подтверждение, что для удовлетворения текущих бизнес-требований, в том числе потребностей в расходах и ожидаемого роста количества пользователей, не нужны механизмы автомасштабирования, а процедуры масштабирования вручную полностью задокументированы и регулярно тестируются.	Да	Да	Нет	Да	
2.3. Осуществляется централизованное управление журналами AWS и приложений	Все содержимое журналов приложений и инфраструктуры AWS следует объединять в одну систему.	Да	Да	Нет	Нет	
2.4. Осуществляется централизованное управление мониторингом AWS и приложений, а	Управление инфраструктурой приложения и AWS необходимо осуществлять централизованно, а сформированные уведомления отправлять соответствующему персоналу, занимающемуся вопросами операционной деятельности.	Да	Да	Нет	Нет	

также уведомлениями						
2.5. Выделение инфраструктуры и управление ею автоматизировано	Для выделения инфраструктуры AWS и управления ею решение должно использовать автоматизированный инструмент, такой как CloudFormation или Terraform. Не следует использовать консоль AWS для внесения рутинных изменений в производственную инфраструктуру AWS.	Да	Да	Нет	Нет	
2.6. Резервное копирование данных выполняется регулярно	Необходимо регулярно выполнять резервное копирование данных в надежную службу хранения. Резервные копии позволяют выполнить восстановление после административных, логических или физических сбоев. Для резервного копирования и архивирования рекомендуется использовать сервисы Amazon S3 и Amazon Glacier. Оба сервиса представляют собой надежные, экономичные платформы хранения. Оба сервиса предлагают неограниченную емкость и не требуют управления объемом или носителями данных по мере роста резервных наборов данных. Благодаря применению модели оплаты по факту использования и низкой стоимости гигабайт-месяца эти сервисы прекрасно подходят для сценариев использования, связанных с защитой данных.	Да	Да	Нет	Нет	
2.7. Тестирование механизмов восстановления осуществляется регулярно, а также после значительных изменений в архитектуре	Тестировать механизмы и процедуры восстановления необходимо как периодически, так и после внесения значительных изменений в облачную среду. AWS предоставляет значительные ресурсы для управления резервным копированием и восстановлением данных.	Да	Да	Нет	Нет	
2.8. Решение устойчиво к прерыванию работы зоны доступности	Решение должно продолжать функционировать в случае, если работа всех сервисов в пределах одной зоны доступности прерывается.	Да	Да	Нет	Да	
2.9. Проверена отказоустойчивость решения	Устойчивость инфраструктуры к прерыванию работы одной зоны доступности проверена в реальных условиях, например в рамках игрового дня, не ранее, чем 12 месяцев назад.	Да	Да	Нет	Да	
2.10. Разработан план аварийного восстановления	Строго определенный план аварийного восстановления включает целевую точку восстановления (RPO) и целевое время восстановления (RTO). Необходимо определить RPO и RTO для всех включенных сервисов. RPO и RTO должны соответствовать соглашению об уровне обслуживания, которое вы предлагаете клиентам.	Да	Да	Нет	Нет	
2.11. Целевое время восстановления (RTO) не превышает 24 часов	Основополагающее требование заключается в том, чтобы RTO базовых сервисов не превышало 24 часов.	Да	Да	Нет	Нет	
2.12. План аварийного восстановления	План аварийного восстановления необходимо проверять на соответствие целевой точке восстановления (RPO) и целевому времени	Да	Да	Нет	Нет	

надлежащим образом проверен	восстановления (RTO) как регулярно, так и после крупных обновлений. До одобрения вашей заявки на присвоение статуса опытного партнера APN необходимо провести по крайней мере одну проверку аварийного восстановления.					
2.13. План аварийного восстановления включает восстановление в другую учетную запись AWS	План аварийного восстановления должен включать стратегию восстановления в другую учетную запись AWS, а при проведении периодического тестирования необходимо проверять этот сценарий. В течение последних 12 месяцев должно быть проведено как минимум одно полное тестирование плана аварийного восстановления, включая по крайней мере восстановление в другую учетную запись AWS. Примечание. Несмотря на то что восстановление данных в тестовые среды или экспортирование данных для пользователей может использоваться для проверки резервного копирования, эти процедуры не удовлетворяют требованию по тестированию полного восстановления в другую учетную запись AWS.	Да	Да	Нет	Нет	
3.0. Оптимизация бизнес-процессов Основополагающие элементы оптимизации бизнес-процессов – эксплуатация и мониторинг систем в целях повышения ценности бизнеса и постоянного совершенствования процессов и процедур. К основным аспектам относятся автоматизация изменений и управление ими, реагирование на события и определение стандартов успешного управления повседневными операциями.						
3.1. Развертывание изменений в коде автоматизировано	Решение должно использовать автоматизированный способ развертывания кода в инфраструктуре AWS. Для развертывания обновлений в инфраструктуре AWS запрещается использовать интерактивные сессии SSH или RDP.	Да	Да	Нет	Нет	
3.2. Определены процедуры Runbook и процедура эскалации	Необходимо разработать набор стандартных процедур Runbook, используемых для реагирования на различные события приложений и AWS. Необходимо определить процедуру эскалации для работы с предупреждениями и уведомлениями, сформированными системой, а также для реагирования на сообщенные клиентами инциденты. Процедура эскалации должна также включать передачу обращений в AWS Support в соответствующих случаях.	Да	Да	Нет	Нет	
3.3. Для учетной записи AWS включена поддержка AWS Support уровня «Для бизнеса»	Необходимо включить поддержку AWS Support уровня «Для бизнеса». Наличие поддержки AWS Support «Для бизнеса» (или более высокого уровня) – это требование партнерской сети AWS к опытным партнерам-технологам APN. Чтобы получить статус опытного партнера, необходимо включить поддержку «Для бизнеса» по крайней мере для одной из учетных записей AWS.	Да	Да	Нет	Нет	