ORACLE

Архитектура безопасности облачной инфраструктуры Oracle

5 марта 2020 г.

ОТКАЗ ОТ ОТВЕТСТВЕННОСТИ

Этот документ предоставляется исключительно для информационных целей, для помощи в планировании внедрения и обновления описанных компонентов продукта. В нем не содержится обязательств по предоставлению каких-либо материалов, программного кода или функциональных возможностей, и на него не следует полагаться при принятии решения о покупке продукта. Разработка, выпуск и время выхода на рынок всех упомянутых компонентов и функций, описанных в этом документе, относятся исключительно к компетенции корпорации Oracle.

ИСТОРИЯ РЕДАКЦИЙ

В этот официальный документ вносились следующие изменения.

ДАТА	РЕДАКЦИЯ
5 марта 2020 г.	Первоначальная публикация

ОГЛАВЛЕНИЕ

Обзор

Облачная инфраструктура Oracle представляет собой предложение категории «инфраструктура как услуга» (IaaS) второго поколения, архитектура которого основана на принципах приоритетного обеспечения безопасности. В число этих принципов входит виртуализация изолированной сети и развертывание на очищенном физическом узле, благодаря чему обеспечивается превосходная изоляция среды заказчика по сравнению с более ранними проектами общедоступного облака и снижается риск таргетированных кибератак.

Облачная архитектура Oracle выигрывает от многоуровневой защиты и операций системы безопасности, которые распространяются от уровня физического оборудования в наших центрах обработки данных до уровня web-доступа, в дополнение к средствам защиты и управления, доступным в нашем облаке. Для обеспечения безопасности современных корпоративных нагрузок и данных в местах их расположения многие из этих средств защиты также работают со сторонними облачными и локальными решениями.

Этот документ содержит сведения о том, как облачная инфраструктура Oracle удовлетворяет требованиям безопасности предприятий и заказчиков для критически важных нагрузок и конфиденциальных данных. Здесь подробно рассказывается о том, какое влияние средства обеспечения безопасности оказывают на архитектуру, проектирование центра обработки данных, подбор сотрудников, а также процессы выделения и использования ресурсов, сертификации и обслуживания облачной инфраструктуры Oracle.

Проектирование по принципу «безопасность прежде всего»

С ростом популярности облака возросла и важность вопросов безопасности. Изначально приоритетной задачей облачной инфраструктуры Oracle было решение проблем безопасности, унаследованных из облаков первого поколения.

Публичные облака первого поколения

В центре внимания публичных облаков первого поколения находилось эффективное использование ресурсов оборудования, осуществлявшееся за счет виртуализации и применения гипервизора. В основе таких облаков лежали многие из тех технологий и принципов, которые используются в частных облаках. Они были спроектированы таким образом для того, чтобы избежать простоев дорогостоящего оборудования. Порой безопасность не являлась основополагающим принципом этого проектирования, поскольку частные центры обработки данных полагались на защиту периметра. С распространением публичных облаков возросла и обеспокоенность в связи с уязвимостями в случае атак на уровне гипервизора. Основной заботой корпоративных заказчиков является безопасность, а риски, связанные с применением гипервизора в публичных облаках первого поколения, только продолжали расти.

Облачная инфраструктура Oracle — публичное облако второго поколения

Перед командой по созданию облачной инфраструктуры Oracle стояла задача разработать публичное облако по принципу «безопасность прежде всего», которое могло бы завоевать доверие организаций и заказчиков, у которых имеются критически важные нагрузки. Принцип *«безопасность прежде всего»* означает, что мы перепроектировали стек виртуализации таким образом, чтобы снизить риск атак на уровне гипервизора и улучшить изоляцию арендаторов. Такая архитектура позволяет защитить арендаторов друг от друга и от поставщика облачных сервисов. В результате было создано *публичное облако второго поколения*, которое оказалось значительно лучше публичных облаков первого поколения. Мы внедрили эту архитектуру в облачную инфраструктуру Oracle во всех центрах обработки данных и регионах.

Облачная инфраструктура Oracle представляет собой полную платформу IaaS. Она предоставляет сервисы, необходимые для создания и запуска приложений в высокозащищенной программно-аппаратной среде с лучшей в отрасли производительностью и доступностью. Вы можете запускать вычислительные сервисы и сервисы баз данных на «голом железе», которое представляет собой выделенные для конкретного заказчика физические серверы, или в виде *экземпляров виртуальных машин (ВМ)*, которые представляют собой изолированные вычислительные среды поверх «голого железа». «Голое железо» и экземпляры ВМ работают на одинаковом серверном оборудовании, программно-аппаратных средствах, базовом ПО и сетевой инфраструктуре, поэтому у экземпляров обоих типов имеются встроенные на этих уровнях средства защиты облачной инфраструктуры Oracle.

БЕЗОПАСНОСТЬ ПЛАТФОРМЫ

Архитектура облачной инфраструктуры Oracle была разработана с целью обеспечения безопасности за счет отдельного уровня виртуализации сети, установки высокозащищенных аппаратных прошивок, контроля физической сети и ее сегментирования.

Отдельный уровень виртуализации сети

Центральное значение в дизайне облачной инфраструктуры Oracle имеет *изоляция виртуализованной сети*, которая значительно снижает риски на уровне гипервизора.

Гипервизор — это ПО, которое управляет виртуальными устройствами в облачной среде, выполняя виртуализацию серверов и сети. В традиционных средах виртуализации гипервизор управляет сетевым трафиком, обеспечивая его передачу между экземплярами ВМ, а также между экземплярами ВМ и физическими узлами. Это повышает сложность и заставляет гипервизор производить дополнительные расчеты. Пробные атаки, такие как выход за пределы виртуальной машины («guest escape»), выявили существенные риски, связанные с таким дизайном. Эти атаки используют в своих интересах сложное устройство гипервизора: злоумышленнику предоставляется возможность «вырваться» из экземпляра ВМ, получить доступ к операционной системе и захватить управление гипервизором. После этого злоумышленник может получить доступ к другим узлам, причем порой ему удается избежать обнаружения.

Облачная инфраструктура Oracle снижает этот риск за счет отсоединения задачи виртуализации сети от гипервизора.
Мы реализовали виртуализацию сети на дополнительном уровне оборудования и ПО, которое забирает управление облаком у гипервизоров и узлов и помещает его в собственную сеть. Именно этот контролируемый усиленный уровень управления делает возможной изоляцию виртуализованной сети.

Отдельный уровень виртуализации сети снижает риск за счет ограничения спектра атак. Даже если злоумышленнику удастся совершить выход за пределы ВМ на одном узле, система спроектирована таким образом, что он не сможет получить доступ к другим узлам в облачной инфраструктуре. Атака успешно сдерживается на одном узле. Виртуализация изолированной сети реализована во всех центрах обработки данных во всех регионах. Это означает, что все арендаторы облачной инфраструктуры Oracle пользуются преимуществами, которые дает снижение такого риска.

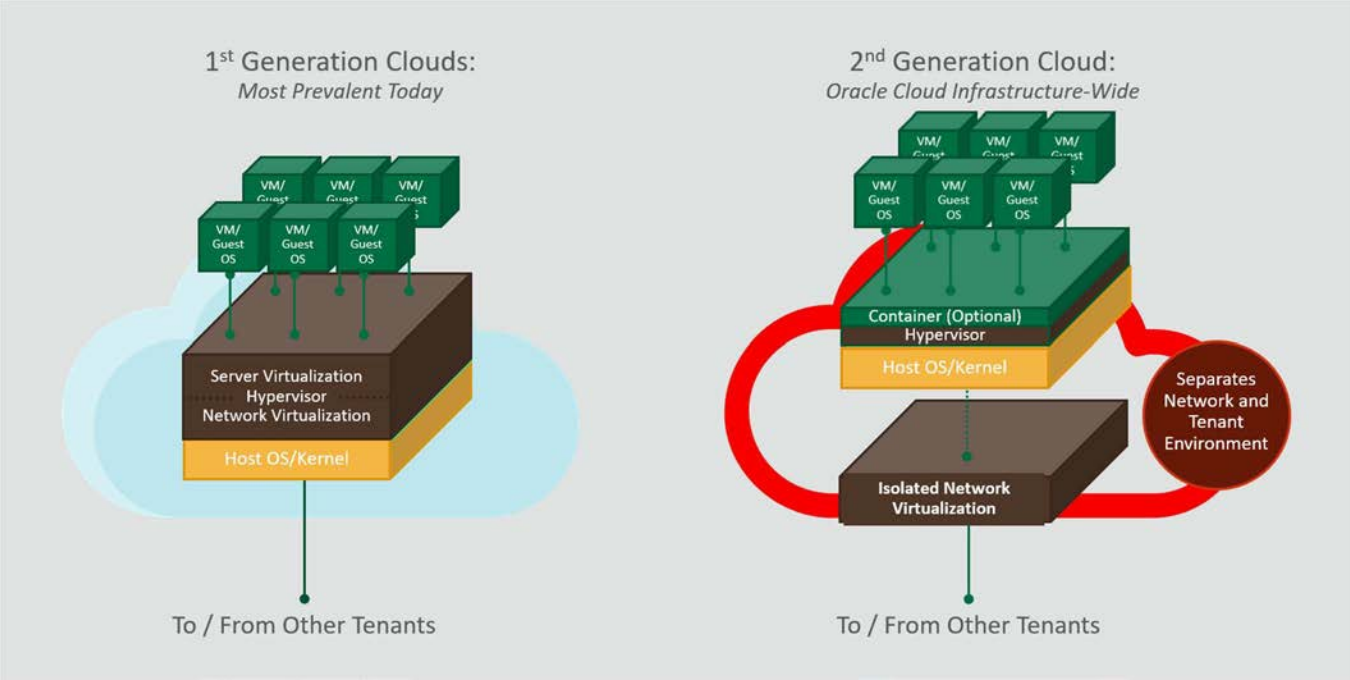

Рис. 1. Отдельный уровень виртуализации сети снижает риск в облаке Oracle второго поколения

Оборудование

Основной принцип дизайна облачной инфраструктуры Oracle — защита арендаторов от атак через скомпрометированные прошивки аппаратного обеспечения. Угрозы на уровне аппаратных прошивок становятся все более распространенными, вследствие чего растут потенциальные риски для поставщиков общедоступных облачных сервисов. Для того чтобы снабдить каждый сервер чистой прошивкой, мы внедрили аппаратные модули доверительной загрузки для процесса стирания и переустановки серверных прошивок. Мы используем этот процесс каждый раз при выделении нового сервера арендатору или ряду арендаторов независимо от типа экземпляра.

Аппаратный модуль доверительной загрузки представляет собой аппаратный компонент, изготовленный в соответствии с нашей спецификацией и проинспектированный визуально. Он предназначен исключительно для выполнения одной задачи, которая заключается в стирании и переустановке программно-аппаратного обеспечения. Он вызывает цикл перезагрузки узла оборудования, запрашивает установку известной аппаратной прошивки и подтверждает выполнение процесса надлежащим образом. Этот способ установки аппаратных прошивок снижает риск атак на уровне прошивок, таких как постоянный отказ в обслуживании (PDoS) или попытки встроить в программно-аппаратное обеспечение инструменты обхода системы защиты для кражи данных или закрытия доступа к ним иным способом.

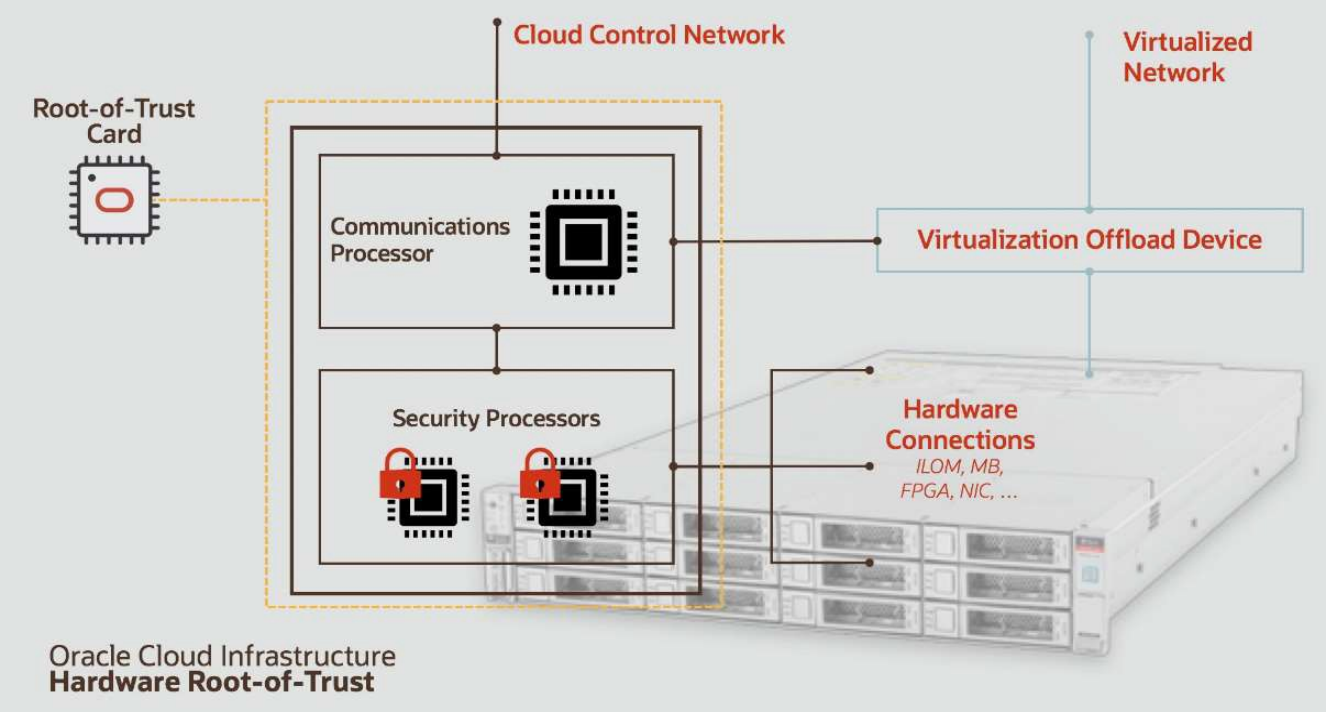

Рис. 2. Дизайн аппаратного модуля доверительной загрузки для установки аппаратных прошивок

Физическая сеть

Архитектура физической сети облачной инфраструктуры Oracle добавляет еще один уровень защиты к изолированной виртуализованной сети путем дальнейшей изоляции объектов аренды заказчиков и ограничения риска распространения угрозы. Компонентами физической сети являются стойки, маршрутизаторы и коммутаторы, которые формируют физический уровень облачной инфраструктуры Oracle.

В коммутаторах агрегации трафика на уровне стойки (top-of-rack, ToR) принудительно применяются списки контроля доступа (ACL). Списки ACL обеспечивают соблюдение путей передачи данных по каналам связи внутри топологии. Например, коммутатор ToR отбрасывает любой пакет, в котором IP-адрес отправителя и соответствующий порт физической сети не совпадают с ожидаемым сопоставлением. Подобное несоответствие возникает в том случае, если злоумышленник подделал виртуальный IP-адрес отправителя с целью выдать себя за надежный источник трафика и получить доступ к другим арендаторам. Списки ACL разработаны таким образом, чтобы предотвратить подделку IP-адресов путем установления соответствия между ожидаемыми IP-адресами

устройства виртуализации изолированной сети и физическими портами, к которым подключено устройство. Кроме того, устройство получателя выполняет для пакетов проверку обратного тракта, чтобы предотвратить искажение инкапсулированного заголовка.

Схема физического уровня проста: плоская сеть подключена к виртуальным портам в виртуальной облачной сети (VCN). Такая схема снижает сложность управления разрешенными трактами передачи трафика и повышает наглядность попыток их обхода.

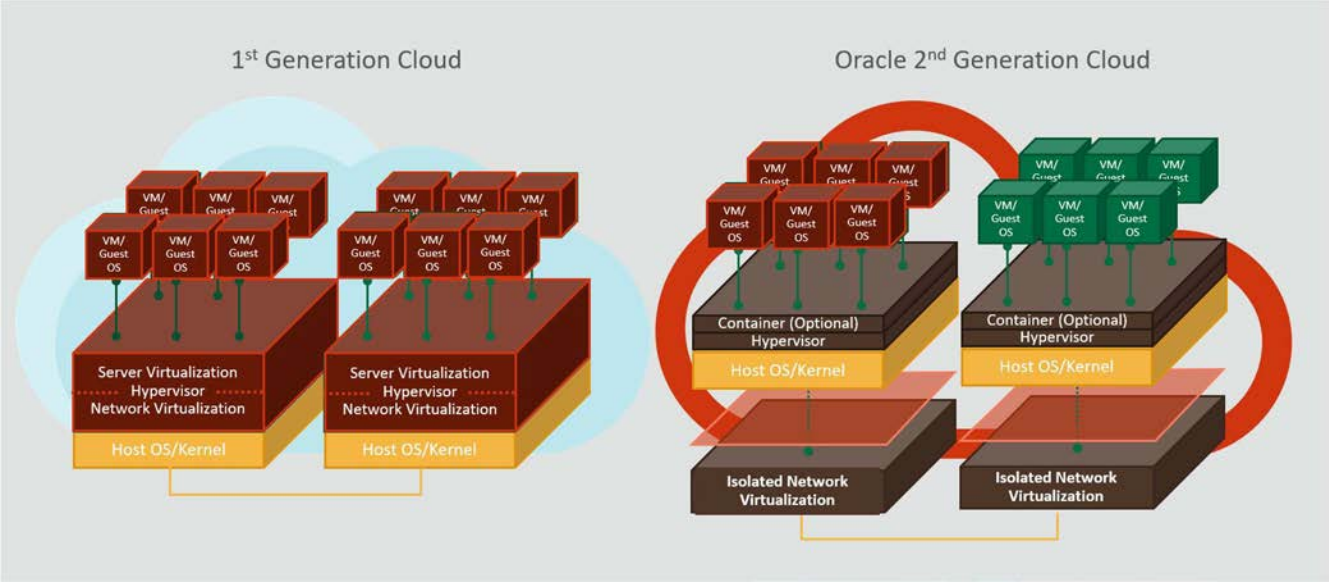

Рис. 3. Простая схема плоской сети защищает облако второго поколения

Сегментирование сети

Физическая сеть облачной инфраструктуры Oracle спроектирована таким образом, чтобы обеспечивать изоляцию заказчиков и сервисов. Она сегментируется на анклавы с уникальными профилями передачи данных. Доступ в эти анклавы и обратно управляется, отслеживается и определяется политиками.

Электропитание вычислительных узлов управляется модулем Integrated Lights Out Manager (ILOM). У каждого узла имеется только один модуль управления ILOM, и обмен данными с другими узлами запрещен. Сеть ILOM принимает командные сообщения только от анклава сервисов, где и происходит выделение ключевых сервисов облачной инфраструктуры Oracle. В число этих сервисов входят Networking, Identity & Access Management (IAM), Block Volumes, Load Balancing и Audit. Для доступа к анклаву сервисов сотрудникам Oracle должны быть предоставлены явные права пользователя, выданные уполномоченными специалистами. Такой доступ регулярно проверяется и пересматривается. Анклавы сервисов находятся на уровне регионов, поэтому весь необходимый трафик между ними проходит через те же механизмы обеспечения безопасности (узлы-бастионы SSH на входе и SSL-прокси на выходе), что и интернет-трафик.

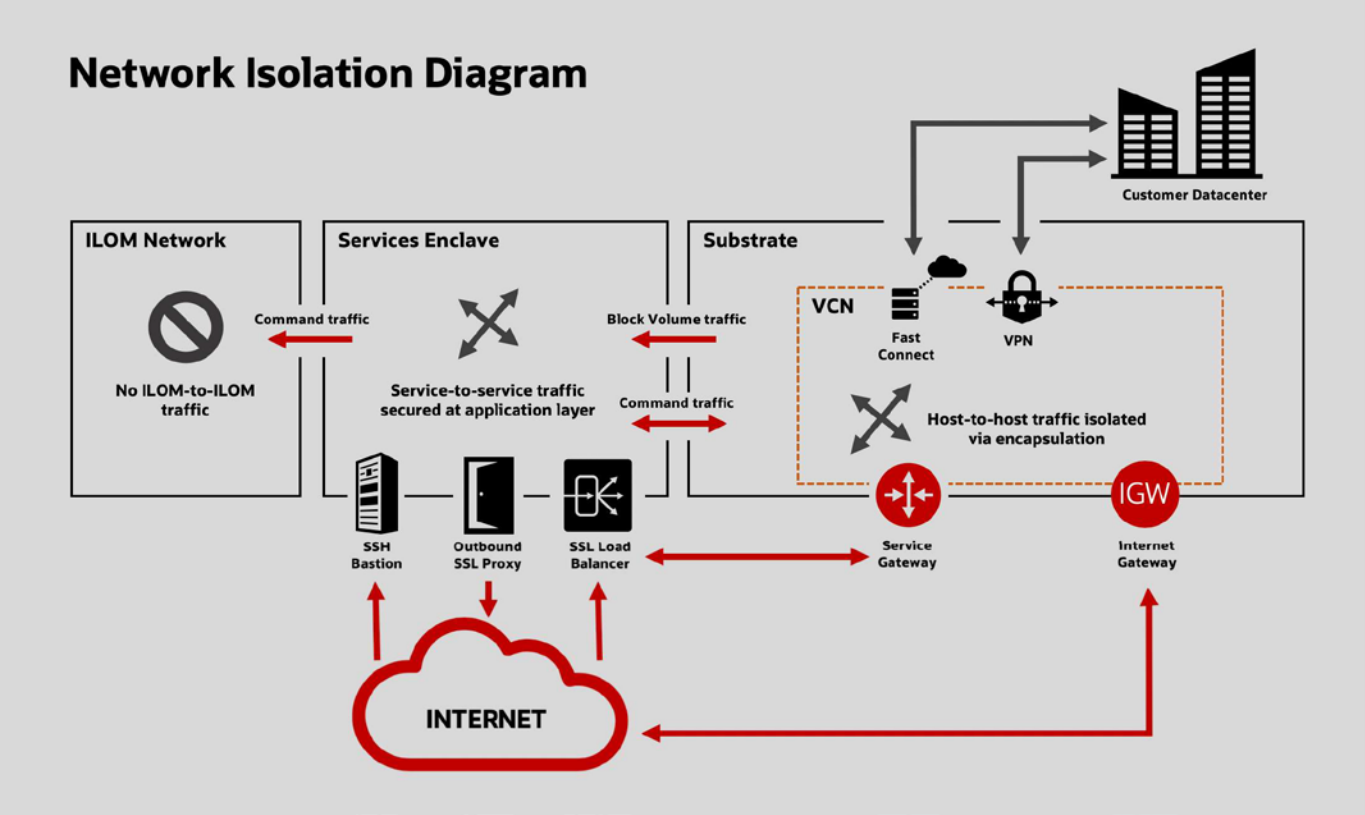

Рис. 4. Сегментирование сети изолирует ресурсы и сервисы заказчика

ОТКАЗОУСТОЙЧИВАЯ ИНФРАСТРУКТУРА

Облачная инфраструктура Oracle разбита по регионам, которые создаются на определенных территориях и включают от одного до трех доменов доступности. Независимо от количества доменов в регионе, где размещены ваши экземпляры, работоспособность и резервное копирование данных и сервисов обеспечиваются несколькими уровнями избыточности.

Отказоустойчивость встроена в архитектуру сервисов и способ хранения данных. Сервисы и данные занимают стойки оборудования, которые включают несколько уровней избыточности на уровне узла, сервера и аппаратных компонентов. Сервисы подключения и пограничные сервисы передачи данных связывают каждый регион с другими регионами, а также с одноранговыми сетями и центрами обработки данных заказчиков.

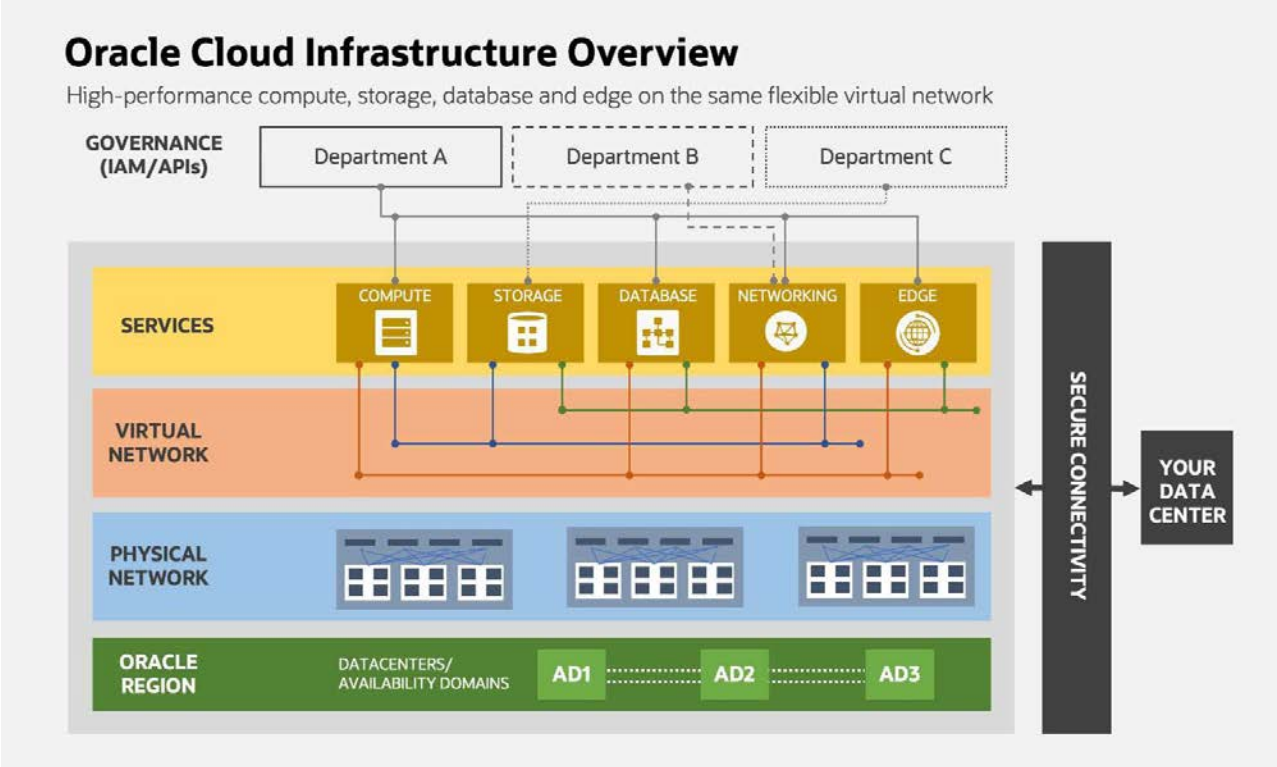

Рис. 5. Отказоустойчивая схема в регионах облачной инфраструктуры Oracle

ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

Объекты, которые потенциально могут стать центрами обработки данных и местоположениями поставщиков облачной инфраструктуры Oracle, проходят широкомасштабный процесс оценивания рисков. В рамках этого процесса рассматриваются такие факторы, как экологические угрозы, доступность и стабильность энергоснабжения, репутация и опыт поставщика, функции соседних объектов и геополитические соображения.

Центры обработки данных обеспечивают соответствие стандартам ANSI/TIA-942-A Tier 3 или Tier 4 Uptime Institute и Telecommunications Industry Association (TIA) и следуют методологии избыточности N2 для эксплуатации критически важного оборудования. Центры обработки данных, в которых размещены сервисы облачной инфраструктуры Oracle, обязаны использовать резервные источники питания и поддерживать генераторы резервного энергоснабжения. Обеспечивается контроль температуры и влажности воздуха в серверных комнатах, которые также оборудованы противопожарными системами. Сотрудники центра обработки данных обучены быстрому реагированию и ознакомлены с процедурами эскалации в случае событий, связанных с безопасностью или доступностью.

Наш многоуровневый подход к обеспечению безопасности центров обработки данных начинается с самого здания. Объекты, в которых находятся центры обработки данных, построены из прочных материалов, таких как железо, бетон и др. Их конструкция должна выдерживать воздействие транспортных средств малой грузоподъемности.

В центрах обработки данных используется периметровое ограждение для защиты объекта снаружи, а сотрудники службы охраны и камеры проверяют транспортные средства. Все, кто входит в центр обработки данных, обязаны пройти через контрольно-пропускные пункты на входе в здание. Любое лицо, у которого отсутствует электронный пропуск, выдающийся на конкретном объекте, должен предъявить удостоверение личности государственного образца и согласованный запрос на доступ в здание. Все сотрудники и посетители обязаны всегда носить официальные именные пропуска. На всех объектах работают охранники.

Дополнительные уровни безопасности между входом на объект и серверными комнатами могут отличаться в зависимости от здания и профиля риска. Сами серверные комнаты должны оборудоваться большим количеством уровней безопасности, в том числе камерами, двухфакторным контролем доступа и механизмами обнаружения вторжения. Физические барьеры от пола до потолка создают изолированные зоны безопасности вокруг серверных и сетевых стоек. Эти барьеры опускаются ниже съемного пола и поднимаются выше потолочной плитки там, где это возможно. Доступ к серверным комнатам предоставляется уполномоченными специалистами только

на требуемый период времени. Использование доступа отслеживается, а доступ, выданный в рамках системы, периодически проверяется и изменяется при необходимости.

БЕЗОПАСНОЕ ПОДКЛЮЧЕНИЕ

Доступ по принципу минимальных прав

Не являющиеся необходимыми или устаревшие права представляют существенную угрозу. Злоумышленники могут получить к ним доступ и использовать их для перемещения в системе. Чтобы сократить риск, исходящий от пользователей или приложений, наделенных чрезмерными правами, при предоставлении доступа к программным комплексам мы руководствуемся принципом минимальных прав. Мы периодически проверяем утвержденные списки членов группы технического обслуживания и отзываем доступ, если реальная необходимость в нем отсутствует.

Для доступа к производственным системам требуется многофакторная аутентификация (MFA). Служба безопасности предоставляет маркеры MFA и отключает маркеры неактивных участников. Весь доступ к программным комплексам записывается в журналы, которые хранятся с целью проведения анализа безопасности.

Несколько уровней аутентификации

Ненадежные учетные данные также представляют существенную угрозу облачным средам. Чтобы усилить аутентификацию, мы используем несколько уровней расширенного контроля доступа для измерения доступа к сетевым устройствам и серверам, поддерживающим эти ресурсы. Один из этих уровней представляет собой обязательное подключение виртуальной частной сети (VPN) к производственной сети. Эта VPN требует большого разнообразия паролей и использования универсальной двухфакторной (U2F) аутентификации, открытого стандарта для усиления и упрощения двухфакторной аутентификации с помощью аппаратного ключа. Все сведения об административном доступе записываются в журналы, а все права доступа проверяются на соответствие принципу минимальных прав. Использование многофакторной аутентификации помогает предотвратить доступ злоумышленника к административной сети из-за ненадежного пароля или его утечки.

Внутреннее подключение

Домены и регионы доступности облачной инфраструктуры Oracle обеспечивают конфиденциальность данных при передаче трафика облачной сети в другие центры обработки данных облачной инфраструктуры Oracle. Эта конфиденциальность достигается за счет частных, выделенных волоконно-оптических соединений глобальной сети (WAN), дальнейшая защита которых обеспечивается путем шифрования MACSec (802.1AE). MACSec представляет собой высокоскоростной протокол сетевого шифрования на уровне 2 модели OCI, который зашифровывает трафик других протоколов уровня 3, не являющихся IP-протоколами, например DNS и ICMP, для которых может отсутствовать традиционное шифрование на уровне 3.

Внешнее подключение

Заказчикам зачастую требуется подключение объекта аренды облачной инфраструктуры Oracle к кампусу, частному центру обработки данных или другим облакам. Мы предлагаем два способа безопасного подключения облачной инфраструктуры Oracle к сетям, не являющимся VCN-сетями.

- IPSec VPN — выделенный шифрованный туннель, который можно проложить в интернете общего пользования.
- FastConnect — частное выделенное высокоскоростное подключение WAN с возможностью выделения туннеля IPSec VPN.

ОПЕРАЦИОННАЯ БЕЗОПАСНОСТЬ

Высококвалифицированные специалисты нашей службы безопасности занимаются обеспечением безопасности облачной инфраструктуры Oracle. В рамках службы безопасности выделено несколько команд, отвечающих за безопасную разработку, мониторинг, тестирование, а также соблюдение требований и соответствие программам сертификации.

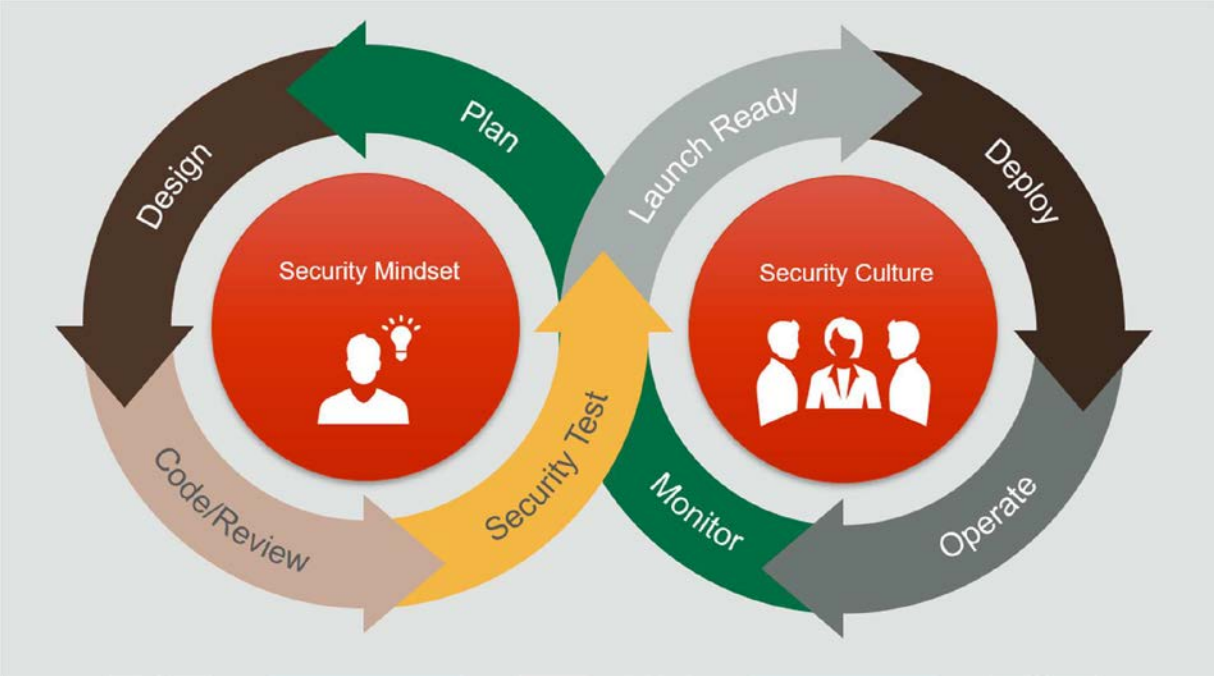

Рис. 6. Обеспечение операционной безопасности облачной инфраструктуры Oracle

Оборонительная безопасность

Сетевая и вычислительная инфраструктура всех вычислительных сред ежедневно подвергается атакам. Для мониторинга этих событий и реагирования на них необходима специальная группа экспертов и аналитиков в области безопасности. В облачной инфраструктуре Oracle этим занимается группа оборонительной безопасности. Специалисты этой группы занимаются оперативным реагированием на нарушение безопасности облака. Они активно и неустанно работают над обнаружением потенциальных угроз и закрытием путей эксплуатации уязвимостей. При обнаружении инцидентов они в кратчайшие сроки устраняют их последствия с помощью современных методологий обеспечения безопасности, а также конфигурации и инструментов DevSecOps.

Агрессивная безопасность

После разработки или изменения какого-либо аспекта архитектуры безопасности облачной инфраструктуры Oracle группа агрессивной безопасности проверяет его на соответствие контрольным показателям и лучшим практикам по безопасности. Специалисты этой группы занимаются изучением и имитацией методов, используемых злоумышленниками, в том числе высококлассными хакерами и государственными службами. В их обязанности входит исследование, тестирование на возможность проникновения и моделирование продвинутых угроз против оборудования и ПО Oracle. Работа группы агрессивной безопасности делает возможными безопасную разработку, создание безопасной архитектуры и расширение оборонительного потенциала.

Обеспечение безопасности

Мы разрабатываем и реализуем планы обеспечения безопасности в соответствии с высокими стандартами безопасности, которые согласуются с существующими стандартами Oracle и отраслевыми стандартами. Чтобы обеспечить безопасность облачной платформы, группа обеспечения безопасности совместно с группами технического обслуживания, а также ключевыми партнерами в области безопасности и рисков в компании Oracle занимается разработкой и развертыванием средств, технологий и процессов обеспечения безопасности, а также указаний для команд специалистов, занимающихся разработкой облачной инфраструктуры Oracle.

ЗАЩИТА ДАННЫХ И ПРИЛОЖЕНИЙ

Способы обработки данных облачной инфраструктуры Oracle и управления ими разработаны таким образом, чтобы обеспечить защиту ваших данных и приложений от внешних угроз.

Доступ к данным

Мы выделяем две широкие категории данных при взаимодействии с заказчиками.

- **Данные о наших заказчиках.** Контактная и прочая связанная информация, необходимая для эксплуатации учетной записи облачной инфраструктуры Oracle и оплаты сервисов. Использование любых персональных данных, которые мы собираем с целью управления учетной записью, регулируется Общей политикой конфиденциальности компании Oracle.
- **Данные, которые хранят наши заказчики.** Данные, которые заказчики хранят в облачной инфраструктуре Oracle, такие как файлы, документы и базы данных. У нас нет информации о содержимом этих данных. Обработка нами этих данных регулируется Политикой конфиденциальности сервисов Oracle и Соглашением об обработке данных для сервисов Oracle.

Уничтожение данных

Мы используем процессы физического уничтожения и логического стирания данных, чтобы не оставлять данные в выведенном из эксплуатации оборудовании.

Уничтожение среды хранения данных

Требования к управлению ресурсами Oracle прямо запрещают удаление средств хранения, содержащих данные заказчика, из серверного зала, в котором они находятся. В каждом серверном зале в центре обработки данных имеется устройство для безопасной утилизации средств хранения. При отказе или выведении из эксплуатации с целью уничтожения жесткий диск или любое другое средство хранения данных помещается на хранение в это устройство для размагничивания и измельчения.

Стирание данных

Когда заказчик освобождает экземпляр BM, API-вызов запускает рабочий процесс по его удалению. Когда новый экземпляр «голого железа» для вычислений добавляется в сервис или освобождается заказчиком или сервисом, оборудование подвергается рабочему процессу обслуживания, прежде чем поступить в запасы для повторного назначения. Этот автоматизированный рабочий процесс обнаруживает физическое средство хранения, подключенное к узлу. Затем рабочий процесс начинает безопасное стирание путем выполнения команды стирания, соответствующей типу средства хранения.

Узлы, предназначенные для использования заказчиками, также оснащены подключенным к сети диском, который используется для кэширования хранилища заказчика. Стирание данных этого диска выполняется с помощью команды безопасного стирания через интерфейс ATA. После завершения процесса стирания запускается процесс перезаписи BIOS, обновления драйверов и возврата оборудования в начальное заводское состояние. Рабочий процесс также проверяет оборудование на наличие неисправностей. Если рабочий процесс не удается выполнить или он обнаруживает неисправность, на узел ставится отметка о необходимости дальнейшего расследования. Когда заказчик прекращает использовать блочное хранилище, ключ удаляется без возможности восстановления, в результате чего данные навсегда становятся недоступны.

Шифрование данных

Мы реализовали программу «повсеместного шифрования» с целью всегда и везде выполнять шифрование всех данных. Шифрование данных заказчика осуществляется как при хранении, так и при передаче. Сервисы Block Volumes и Object Storage по умолчанию включают шифрование данных при хранении с помощью алгоритма Advanced Encryption Standard (AES) с 256-битным шифрованием. Шифрование передаваемых в систему управления данных осуществляется с использованием протокола безопасности транспортного уровня (TLS) 1.2 или более поздней версии.

Безопасность API

В современных облачных средах интерфейсы API крайне важны для функционирования приложения. Однако они также открывают более широкий спектр атак. Мы понимаем важность безопасности API для приложений в облачных средах, поэтому разработали сервис API Gateway для защиты API.

API Gateway — это полностью управляемый региональный сервис, который интегрируется с сетями заказчиков в облачной инфраструктуре Oracle. Шлюзы API дают заказчикам возможность публиковать общедоступные или частные API-интерфейсы, обрабатывать входящие запросы заказчиков, а также применять политики безопасности, доступности и подтверждения. Кроме того, шлюзы API перенаправляют запросы бэкенд-сервисам, применяют политики к ответам от этих сервисов, а затем перенаправляют ответы клиенту. Шлюзы API защищают и изолируют бэкенд-сервисы и помогают заказчикам применять метрики к вызовам API.

Для обеспечения конфиденциальности и целостности данных соединения между клиентами и шлюзами API всегда используют протокол TLS. Заказчики также могут настраивать использование протокола TLS в соединениях между шлюзами API и бэкенд-сервисами.

КУЛЬТУРА ДОВЕРИЯ И СООТВЕТСТВИЯ ТРЕБОВАНИЯМ

Все практики в облачной инфраструктуре Oracle базируются на более широкой культуре доверия и соответствия требованиям.

Безопасность разработки

Oracle Software Security Assurance (OSSA) — это методология компании Oracle по встраиванию средств обеспечения безопасности на фазах проектирования, создания, тестирования и сопровождения продуктов независимо от того, используются ли они заказчиками локально или предоставляются в Oracle Cloud. Наша цель — помочь заказчикам обеспечить выполнение требований к безопасности по доступной цене. Лучшие в отрасли стандарты, технологии и практики OSSA преследуют следующие цели.

- **Содействие развитию инноваций в сфере обеспечения безопасности.** Нашу давнюю традицию внедрения инноваций в сфере обеспечения безопасности продолжают решения, позволяющие организациям реализовывать согласованные политики безопасности в рамках гибридных облачных центров обработки данных и управлять ими. В число этих решений входит управление безопасностью баз данных и идентификационными данными, а также мониторинг и анализ безопасности.
- **Сокращение количества недостатков системы безопасности во всех продуктах Oracle.** В программы OSSA входят стандарты защитного кодирования, обязательная подготовка по вопросам безопасности для разработчиков, воспитание лидеров по безопасности в группах разработки, а также использование автоматизированных инструментов анализа и тестирования.
- **Сократить влияние недостатков системы безопасности в выпущенных продуктах.** Мы внедрили прозрачные политики обнаружения и устранения уязвимостей системы безопасности. Мы одинаково относимся ко всем заказчикам и успешно обеспечиваем установку исправлений системы безопасности в рамках программ критических обновлений и оповещений системы безопасности.

Безопасность персонала

Мы стремимся нанимать лучших кандидатов, а затем вкладывать силы в развитие сотрудников. Все сотрудники проходят базовую подготовку по вопросам безопасности. Кроме того, мы даем возможность пройти специализированное обучение для ознакомления с новейшими технологиями, разработками и методологиями в сфере обеспечения безопасности. Мы предлагаем стандартные программы корпоративного обучения, в рамках которых рассматриваются вопросы информационной безопасности и конфиденциальности. Кроме того, мы взаимодействуем с группами специалистов в различных отраслях и отправляем сотрудников на профессиональные конференции для совместной работы над возникающими проблемами со специалистами из других отраслей. Цели программ подготовки по вопросам безопасности компании Oracle — помочь сотрудникам обеспечить безопасность своих продуктов и заказчиков, дать им возможность получить более подробную информацию по интересующим их сферам обеспечения безопасности, а также выполнять свою миссию по привлечению и удержанию лучших специалистов.

Кроме того, мы стремимся принимать на работу людей, неукоснительно соблюдающих этические нормы и способных трезво оценивать ситуацию. Все сотрудники проходят проверку до приема на работу в установленных законом пределах, в том числе проверку на наличие судимости и подтверждение предыдущей занятости в соответствии с действующими в стране правилами найма. Мы выполняем оценку эффективности работы с целью поощрения сотрудников за хорошие результаты и выявления возможностей для развития. Мы используем безопасность в качестве компонента процессов оценки группы. Такой подход позволяет получить представление о том, насколько работа групп соответствует нашим стандартам безопасности, а также определить лучшие практики и области усиления подотчетности при работе с критически важными процессами обеспечения безопасности.

Безопасность цепочки поставок

Мы давно занимаемся разработкой защищенного оборудования корпоративного класса. Выделенная группа специалистов занимается проектированием и тестированием безопасности оборудования, которое используется для обеспечения работоспособности сервисов облачной инфраструктуры Oracle. Эта группа работает совместно с нашей службой снабжения и проверяет аппаратные компоненты на соответствие строгим стандартам обеспечения безопасности.

Соответствие нормативным требованиям

Мы продолжаем вкладывать средства в сервисы, которые позволяют нашим заказчикам с меньшими усилиями обеспечить соответствие требованиям к безопасности и нормативным требованиям. Независимые гарантии способствуют укреплению доверия во взаимоотношениях со сторонними поставщиками услуг. Для завоевания этого доверия мы используем множество постоянных программ, в рамках которых обеспечиваем соответствие глобальным, региональным и отраслевым сертификациям, а также выпускаем отчеты, демонстрирующие это соответствие. Эти отчеты могут сыграть важную роль в управлении компаниями заказчиков, процессах управления рисками, программах управления поставщиками, а также надзоре со стороны контролирующих органов. Кроме того, благодаря применению облачных технологий DevOps мы можем унифицировать обеспечение соответствия сервисов нормативным требованиям, действующих в различных регионах мира, за счет их автоматизированного развертывания.

Аудит

Мы регулярно проводим тестирование на возможность проникновения, тестирование на наличие уязвимостей и оценки безопасности для облачной инфраструктуры, платформенных сервисов и приложений Oracle. Эти тесты призваны проверить и улучшить общую безопасность облачных служб Oracle.

Мы привлекаем независимых аудиторов и оценщиков, чтобы они провели тестирование и высказали свое мнение касательно средств управления безопасностью, конфиденциальностью и доступностью в соответствии с законами, регламентами и отраслевыми стандартами защиты данных.

Мы также разрешаем заказчикам проводить тестирование объекта аренды самостоятельно или с привлечением третьих лиц, как указано в Политике тестирования безопасности.

ЗАКЛЮЧЕНИЕ

Обеспечению безопасности критически важных рабочих нагрузок в облачной инфраструктуре Oracle 2-го поколения уделяется особое внимание. Заказчикам, у которых есть конфиденциальные нагрузки, например финансовые приложения или приложения обслуживания населения, облачная инфраструктура Oracle предоставляет прорывную архитектуру безопасности, которая позволяет уменьшить риски и спектр атак, которые обычно ассоциируются с облаками первого поколения. Мы встроили средства обеспечения безопасности в архитектуру, дизайн центра обработки данных, порядок подбора сотрудников, а также процессы выделения и использования ресурсов, сертификации и обслуживания облачной инфраструктуры Oracle. Это современное публичное облако, созданное для обработки данных, обеспечение безопасности которых требует самых жестких мер.

СВЯЗАТЬСЯ С НАМИ

Позвоните по номеру +7 (495) 641-14-00 или посетите сайт oracle.com/ru.
Если вы находитесь за пределами Северной Америки, найдите местный офис на странице oracle.com/contact.

blogs.oracle.com facebook.com/oracle twitter.com/oracle

Архитектура безопасности облачной инфраструктуры Oracle
Март 2020 г.