ORACLE CLOUD

Безопасность облачных сервисов Oracle Cloud Services для инфраструктур и платформ

ТЕХНИЧЕСКАЯ ПУБЛИКАЦИЯ ORACLE | МАРТ 2016

ORACLE

Отказ от ответственности

Ниже дается описание общего направления развития продукта. Документ может быть использован только в ознакомительных целях и не предназначен для составления какого-либо договора. Он не содержит обязательств по поставкам каких-либо материалов, программного кода или функциональных возможностей и не должен использоваться для принятия решения о покупке. Указание на разработку, версию и время внедрения средств и функциональных возможностей продуктов Oracle в информационных презентациях остается на усмотрение Oracle.

Содержание

Согласно последнему прогнозу Gartner, общие затраты на IaaS в 2015 г. предположительно составят около 16,5 млрд долларов, что на 32,8 % больше по сравнению с 2014 г., а совокупный среднегодовой темп роста за период с 2014 по 2019 г. составит 29,1 %. [http://www.gartner.com/newsroom/id/3055225]

СЬЮЗАН МУР, КОМПАНИЯ GARTNER

1. Введение

Общие затраты на технологию «инфраструктура как услуга» (IaaS) быстро растут. Однако многие руководители ИТ-службы не торопятся полностью переходить на облачные инфраструктуры и платформы услуг. Их медлительность объясняется беспокойством за безопасность корпоративных систем и данных. Руководители ИТ-службы хотят строить гибридные облачные решения, одновременно обеспечивая необходимые меры для защиты всех корпоративных данных. Правильно подобранные решения и процессы по обеспечению безопасности позволяют с уверенностью перейти на облачные вычисления даже предприятиям с самыми высокими требованиями.

Решения Oracle Cloud были разработаны с целью обеспечить безопасность для инфраструктур и платформ, используемых заказчиками Oracle для выполнения критически важных рабочих нагрузок и хранения данных. Почему заказчики Oracle выбирают наши облачные решения? Ответ прост. Заказчики Oracle получают уникальные преимущества, которые нельзя получить у других поставщиков.

» Oracle располагает наиболее полным портфелем самых разнообразных и эффективных интегрированных услуг для инфраструктур и платформ.
» Oracle Cloud позволяет создавать гибридные облака, обеспечивая простое управление и мониторинг из локальных систем и удобный перенос рабочих нагрузок.
» Облачные решения Oracle созданы на основе знакомых заказчикам стандартизированных технологий.

В данном техническом документе рассматриваются общие и специализированные возможности по обеспечению безопасности для следующих сервисов: Oracle Compute Cloud Service, Oracle Storage Cloud Service, Oracle Network Cloud Service, Oracle Java Cloud Service и Oracle Database Cloud Service — Enterprise Edition.

Полный список доступных облачных сервисов Oracle см. по ссылке https://www.oracle.com/cloud.

Заказчикам Oracle Cloud в первую очередь необходимы следующие возможности.

- **Контроль**. Механизмы безопасности, позволяющие контролировать, кто и при каких условиях может получить доступ к данным.
- **Аудит**. Проверка ресурсов с целью поддержания актуальных настроек безопасности.
- **Прозрачность**. Журналы, обеспечивающие прозрачность использования учетных записей и ресурсов.

- **Гарантия**. Независимая проверка порядка, в котором осуществляется хранение данных, доступ к ним и их защита, с целью предотвращения несанкционированного доступа и изменения.
- **Безопасность**. Безопасные разработка, кодирование, тестирование, развертывание и управление для сервиса.
- **Гарантированная интеграция с существующими технологиями Oracle**. Гладкая интеграция с существующими решениями Oracle, такими как управление идентификаторами и доступом.

Безопасность — главный приоритет облачных решений Oracle. Целью Oracle является создание максимально безопасных и надежных услуг для инфраструктур и платформ на основе публичного облака, предназначенных для коммерческих и государственных организаций. Миссия Oracle — строить безопасные сервисы инфраструктур и платформ в публичном облаке, где заказчикам Oracle обеспечивается надежная и управляемая безопасность для уверенного выполнения рабочих нагрузок и создания доверенных масштабируемых облачных решений.

В компании Oracle существует развитая культура безопасности и официальные политики безопасности. На протяжении более чем тридцати лет продукты Oracle использовались коммерческими и государственными организациями во всем мире для запуска критически важных приложений.

Философия безопасности Oracle строится на следующих подходах.

- Разработанная Oracle стратегия предотвращения несанкционированного доступа основана на принципе эшелонирования. Мы считаем, что нужно снизить барьер по периметру и добавить средства для управления безопасностью ближе к данным.
- В дополнение к эшелонированной стратегии Oracle продолжает проектировать мощные и эффективные процессы для обнаружения, реагирования на инциденты несанкционированного доступа и их нейтрализации.
- В настоящее время Oracle работает над моделями обеспечения безопасности и доверия, хорошо совместимыми с облаком. Например, специалисты Oracle полагают, что традиционная модель администрирования, основанная на концепции всемогущего, наделенного всевозможными привилегиями администратора, должна быть заменена моделью с более широкими полномочиями заказчика. Oracle должна управлять только объектами инфраструктуры и не иметь каналов доступа к данным заказчика.

В Oracle работают одни из лучших в мире специалистов по обеспечению безопасности информации, баз данных, приложений, инфраструктур и сетей. Со времени основания корпорация Oracle является ведущей силой в сфере разработки безопасных приложений и систем. Мы используем этот опыт для разработки полнофункциональных облачных решений.

Сервисы Oracle Cloud используются организациями по всему миру, от крупных компаний и госорганизаций, предъявляющих высочайшие требования к безопасности, до предприятий малого

бизнеса. Oracle Cloud предлагает комплексный портфель услуг для IaaS и PaaS, который состоит из услуг вычислительных, хранения данных, сетевых, СУБД, Java, процессных, мобильных, управления данными и бизнес-аналитики. Все созданные Oracle сервисы IaaS и PaaS имеют общий набор функций для обеспечения безопасности, например средства управления идентификаторами и доступом.

2. Oracle Cloud Services: веб-сервисы, которым доверяют

Миссия Oracle состоит в том, чтобы с помощью Интернета дать заказчикам возможность использовать новейшие корпоративные технологии и бизнес-приложения в любой точке земного шара. Oracle Cloud — обширный набор интегрированных сервисов на основе отраслевых стандартов, обеспечивающий доступ на основе подписок к сервисам Oracle для платформ, приложений и социальных сетей. Все сервисы размещены в системах Oracle, находятся под нашим управлением и обеспечиваются полной поддержкой.

Oracle Cloud IaaS предоставляет набор базовых функций для инфраструктуры, таких как эластичные вычисления и хранилище, что дает заказчикам возможность выполнять любые рабочие нагрузки в облаке. Три основные функции Oracle Cloud IaaS позволяют заказчикам создавать виртуальные среды, приложения и связанные конфигурации и управлять ими.

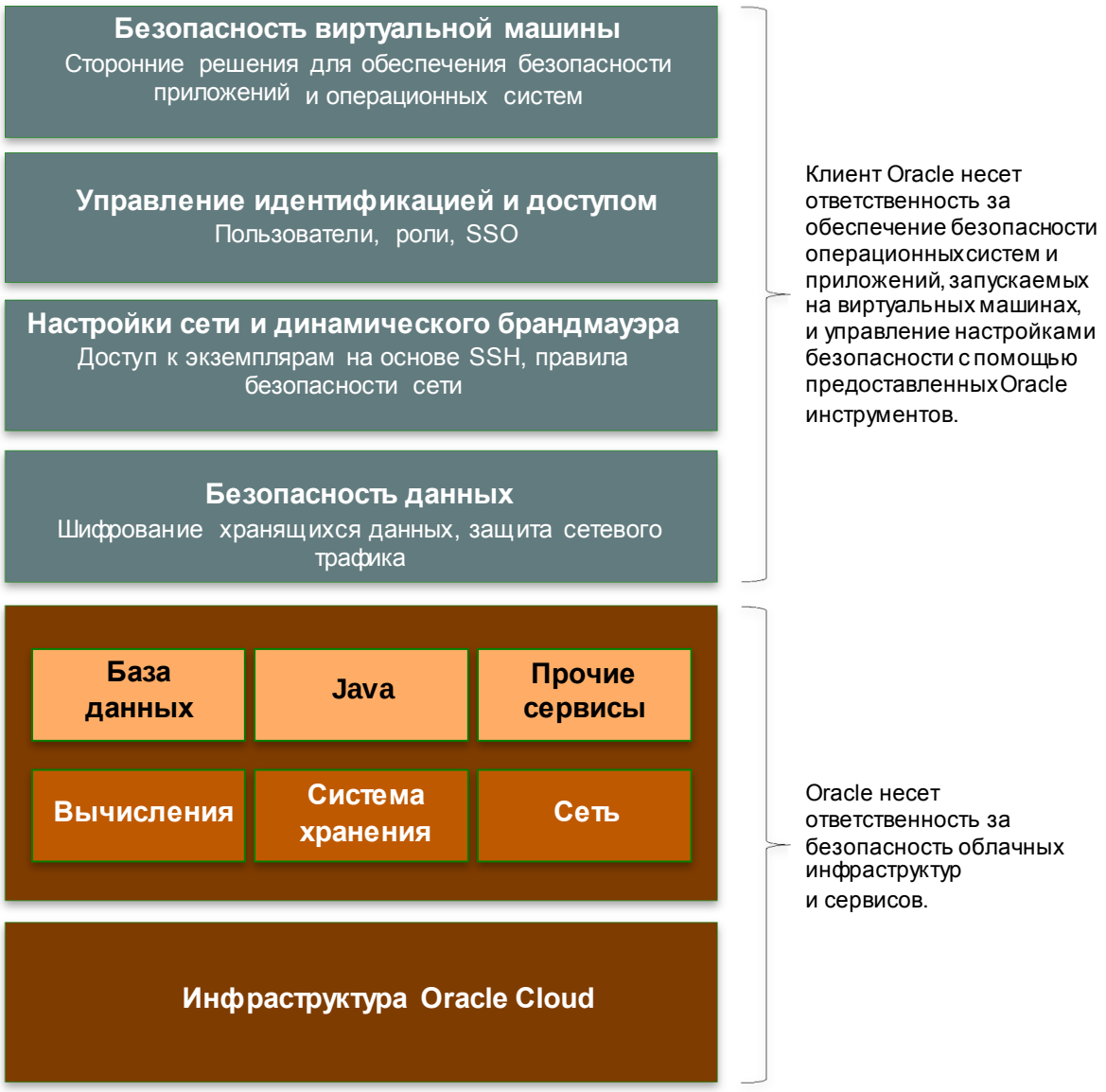
» Oracle Compute Cloud Service предоставляет гибкие возможности для масштабируемых вычислений, блочного хранения данных и сетевых сервисов в Oracle Cloud. Заказчики могут выбирать между мультиарендными эластичными вычислениями или выделенным сервисом для вычислений. При выборе последнего варианта предоставляется вычислительная среда с изолированными вычислительными ресурсами. Благодаря полной сетевой изоляции все вычислительные ресурсы находятся в полном распоряжении заказчика. Заказчики могут получать доступ к Oracle Compute Cloud Service посредством Representational State Transfer (REST) API, интерфейса командной строки (CLI) и пользовательского веб-интерфейса.
» Oracle Storage Cloud Service — экономичное решение для удаленного резервного копирования и архивирования корпоративных данных и приложений. Заказчики могут получить доступ к Oracle Storage Cloud Service с помощью стандартизированного OpenStack REST API, совместимого со Swift, NFSv4 через Oracle Storage Cloud Software Appliance, программным способом с помощью Java API или посредством других сертифицированных приложений сторонних разработчиков. Заказчики также могут отслеживать ключевые показатели системы хранения и управлять пользователями и ролями с помощью графической веб-консоли. В качестве дополнительных мер безопасности заказчики со своей стороны могут использовать возможности шифрования, доступные через программную платформу и библиотеку Java, для шифрования всех объектов с помощью уникальных симметричных ключей перед загрузкой и сохранением объекта в облачном сервисе.
» Oracle Network Cloud Service предлагает два решения на основе VPN. VPN типа «сеть-сеть» для выделенных вычислений позволяет заказчикам подключать ЦОД к Oracle Cloud через туннель IPSec. Второе решение VPN предоставляется через сервис Corente Cloud Services Exchange, в которой используется распределенная виртуальная платформа на границе сети. Помимо решений на основе VPN, заказчики Oracle могут использовать решение Oracle FastConnect, которое создает выделенное соединение с высокой пропускной способностью между клиентскими ЦОД и Oracle Cloud, обеспечивая более предсказуемую производительность сети. FastConnect также предоставляет предварительно заданный путь для передачи данных, в отличие от сети Интернет, таким образом повышая безопасность, так как данные никогда не покидают доверенных границ.

Oracle Cloud PaaS помогает корпоративным отделам ИТ и независимым разработчикам программного обеспечения быстро разрабатывать и развертывать многофункциональные приложения или использовать программное обеспечение Oracle Cloud как приложения SaaS

благодаря облачной платформе корпоративного класса, созданной на основе лучших в отрасли СУБД и сервера приложений. Oracle Cloud PaaS включает в себя множество облачных сервисов, предоставляющих функционал для баз данных на основе СУБД Oracle Database и программно-аппаратного комплекса Oracle Exadata Database Machine. Oracle Java Cloud Service на основе Oracle WebLogic Server обеспечивает платформу поверх облачной инфраструктуры Oracle корпоративного класса для разработки и запуска новых или существующих приложений Java EE. Полный список доступных облачных сервисов Oracle см. по ссылке https://www.oracle.com/cloud.

3. Ответственность заказчиков и компании Oracle при обеспечении безопасности

Используемые вами сервисы определяют, какие работы по конфигурации необходимо выполнить в рамках ваших обязательств по обеспечению безопасности. Сервисы Oracle Cloud для инфраструктур и платформ функционируют в соответствии с моделью общей ответственности, где Oracle несет ответственность за безопасность лежащей в основе облачной инфраструктуры, а вы — за безопасность нагрузок, а также сервисов платформ, таких как Oracle Database и Oracle WebLogic Server. На рисунке ниже приведена схема распределения обязанностей.



Вы должны обеспечить защиту учетных данных для доступа ко всем сервисам Oracle Cloud и создать индивидуальные учетные записи для всех пользователей. Вы несете ответственность за управление доступом к учетным записям ваших сотрудников и проверку возможности получения такого доступа, а также за все действия, совершаемые под такими учетными записями.

Сервисы Oracle Cloud Services, относящиеся к категории IaaS, такие как Oracle Compute Cloud Service и Oracle Storage Cloud Service, находятся под полным управлением заказчика, таким образом вы обязаны обеспечивать выполнение всех необходимых настроек и административных обязанностей. Например, при использовании Oracle Compute Cloud Service вы несете полную ответственность за настройку, функционирование, обслуживание и безопасность операционных систем и иного ПО, использующихся в ваших облачных сервисах, в том числе приложений. Вы несете полную ответственность за выполнение необходимых действий по обеспечению безопасности и защиты контента, его архивированию и резервному копированию, включая использование приложений или технологий шифрования для защиты от несанкционированного доступа. Вы определяете время для установки обновлений. При использовании Oracle Storage Cloud Service вы несете ответственность за шифрование данных со своей стороны перед их загрузкой в Oracle Storage Cloud Service.

Сервисы Oracle Cloud, относящиеся к категории PaaS, такие как Oracle Database Cloud Service и Oracle Java Cloud Service, находятся под полным управлением заказчика. Это означает, что вы должны выполнять все необходимые действия по настройке безопасности и управлению. Например, при использовании Oracle Database Cloud Service вы несете ответственность за резервное копирование, восстановление, обновление и масштабирование с помощью инструментов, предоставляемых Oracle. Вы также несете ответственность за определение политик сетевой безопасности на уровне виртуальных машин, а также правил доступа к базам данных, поскольку вы имеете полные права доступа к экземплярам своих виртуальных машин и баз данных, запускаемых на этих машинах. По умолчанию данные заказчика зашифрованы в табличных пространствах.

При использовании Oracle Java Cloud Service заказчики несут ответственность за резервное копирование, восстановление, обновление и масштабирование с помощью инструментов, предоставляемых Oracle. При использовании версии Oracle Java Cloud Service без виртуального образа Oracle обеспечивает автоматическое резервное копирование.

Oracle несет ответственность за защиту глобальной инфраструктуры, в которой запускаются все сервисы Oracle Cloud. Эта инфраструктура состоит из аппаратного и программного обеспечения, сети и производственных помещений для запуска сервисов Oracle Cloud. В следующих разделах мы подробнее рассмотрим возможности обеспечения безопасности для инфраструктуры и сервисов Oracle.

4. Безопасность облачной инфраструктуры Oracle

Инфраструктура публичного облака Oracle используется для предоставления различных сервисов SaaS, PaaS и IaaS. Она включает в себя производственные помещения, сетевое, аппаратное и программное обеспечение, обеспечивающие работу сервисов. Облачная инфраструктура предназначена для того, чтобы обеспечивать безопасность сервисов для инфраструктур и платформ, которые используются заказчиками Oracle для выполнения критически важных корпоративных рабочих нагрузок и хранения данных. Благодаря сервисам Oracle для вычислений, систем хранения, сети и платформ, запускающимся в одной из самых безопасных облачных инфраструктур, вы сможете создавать масштабируемые корпоративные облачные решения.

4.1. Физические меры безопасности

Oracle использует защищенные помещения как для офисов, так и для рабочей облачной инфраструктуры. Наши центры обработки данных обеспечивают высочайшую производительность благодаря инновационному техническому подходу. По внешнему периметру всех ЦОД находятся бетонные барьеры, перекрывающие проезд транспортным средствам, системы видеонаблюдения, системы охранной сигнализации, а также посты физической охраны. Все эти меры предназначены для защиты от нападений без проникновения. Для получения доступа в ЦОД сотрудники должны пройти двухфакторную аутентификацию.

Доступ в центры обработки данных и к хранящейся в них сведениям предоставляется только сотрудникам и подрядчикам в случае обоснованной рабочей необходимости. Все случаи физического доступа к ЦОД со стороны сотрудников Oracle вносятся в журнал и регулярно проверяются. Входы охраняются 24 часа в сутки, 365 дней в году сотрудниками службы безопасности, которые проводят визуальную проверку личности и организуют сопровождение посетителей.

4.2. Доступ к сервисам Oracle Cloud Services со стороны сотрудников Oracle

Доступ к облачным системам разрешен только авторизованным сотрудникам. Для предоставления доступа используются защищенный туннель VPN с мультифакторной аутентификацией, а также политики доступа к системам управления компонентами инфраструктуры и облаком в среде Oracle Cloud. Средства управления доступом к системе включают в себя системную аутентификацию, авторизацию, получение подтверждения доступа, подготовку данных и отзыв полномочий для сотрудников Oracle и других пользователей, определенных Oracle. Все действия пользователей, включая нажатия клавиш, записываются, чтобы можно было провести аудит и расследование.

Сетевые и системные учетные записи сотрудников Oracle регулярно проверяются, чтобы гарантировать соответствие уровня доступа. При увольнении сотрудника предпринимаются мгновенные меры по прекращению сетевого, телефонного и физического доступа.

4.3. Проверка биографических данных

Для новых сотрудников перед приемом на работу в подразделения Oracle на территории США выполняется проверка личных данных на наличие правонарушений в объемах, разрешенных законодательством. Возможности Oracle для выполнения проверки личных данных на наличие правонарушений в других странах определяются местным законодательством и правилами локального подразделения Oracle.

4.4. Меры для минимизации рисков со стороны сотрудников

Меры для минимизации рисков, связанных с человеческими ошибками, кражей, мошенничеством и ненадлежащим использованием рабочих помещений, включают в себя проверку персонала, заключение соглашений о неразглашении, обучение принципам безопасности, а также применение дисциплинарных взысканий. Сотрудники Oracle должны охранять конфиденциальность данных заказчика. Сотрудники Oracle обязаны подписать соглашение о неразглашении конфиденциальной информации и соблюдать политики компании по защите конфиденциальной информации (кодекс деловой этики и поведения, правила надлежащего использования корпоративных ресурсов и политику защиты информации) в рамках условий трудоустройства. Oracle в письменном виде заключает соглашение о неразглашении конфиденциальной информации со всеми подрядчиками до оказания ими услуг.

4.5. Разделение в корпоративной сети Oracle

Служебная сеть Oracle Cloud отделена от корпоративной сети Oracle и требует отдельный набор учетных данных для получения доступа. Разработчики и администраторы, имеющие доступ к корпоративной сети, должны в письменном виде запрашивать учетные данные для получения доступа к компонентам Oracle Cloud. Все запросы проверяются и подтверждаются соответствующим ответственным лицом.

4.6. Безопасная сетевая архитектура

Сеть Oracle Cloud обеспечивает значительную защиту от традиционных проблем безопасности, таких как DDoS-атаки, атаки с перехватом, подмена IP-адреса и сканирование портов.

Oracle использует устройства сетевой защиты, в том числе брандмауэры, для мониторинга сетевых коммуникаций и управления ими как на внешних, так и внутренних границах сети. Эти устройства используют политики транспортных потоков или списки контроля доступа (ACLs) для управления потоками трафика. Брандмауэры развертываются с использованием многоуровневого подхода, чтобы выполнять пакетную проверку с помощью политик безопасности, настроенных для фильтрации пакетов по протоколу, порту, источнику и IP-адресу с целью определения санкционированных источников, мест назначения и видов трафика. Сервисы Oracle Cloud используют инструменты для оценки сети на наличие угроз безопасности и уязвимостей. Для оценки, проверки, приоритизации и устранения найденных проблем введены специальные процедуры. Корпорация Oracle подписана на системы уведомлений об уязвимостях, чтобы получать сведения об инцидентах безопасности, рекомендации и т. п.

Если наличие рисков или угроз подтверждается, а рекомендуемые изменения применимы для сервисов и не влияют на их функционирование, Oracle предпринимает соответствующие меры.

Меры по защите от DDoS-атак и смягчения их последствий реализуются прежде всего с помощью сертифицированной платформы-брандмауэра с выделенной DOS-защитой. Устройства масштабируются, чтобы поддерживать большие объемы трафика и не терять соединение. Это обеспечивает защиту от атак на уровне 3–7 модели OSI. Даже если атака является широкомасштабной и злоумышленники пытаются создать нагрузку, превышающую пропускную способность каналов связи, или фальсифицируют подлинные подключения, пытаясь исчерпать объем памяти, природа среды для распределения нагрузки с использованием посредника позволяет изучать каждое подключение и реагировать на них, принимая или прекращая подключения в зависимости от ситуации. Эти устройства активно анализируют все сеансы, проверяя протоколы, содержимое и брандмауэр веб-приложений (уровень 7). В этих устройствах используются также такие технологии, как шифрование файлов SYN-cookie, таблицы соединений большой емкости, поиск по шаблонам, проверка потоков, предотвращение затопления пакетами ICMP и TCP-переадресация в порядке поступления.

Сервисы Oracle Cloud Services используют системы обнаружения вторжения в сеть (NIDS) для защиты среды. Датчики NIDS развертываются в сети в режиме предотвращения вторжений (IPS) или обнаружения вторжений (IDS), чтобы отслеживать и блокировать подозрительный трафик, не пропуская его во внутреннюю сеть. Уведомления NIDS направляются в централизованную систему мониторинга, которая находится под управлением групп по обеспечению безопасности круглосуточно и без выходных.

4.7. Зашифрованный доступ к сервисам Oracle Cloud Services

Обычно заказчики получают доступ к системе через Интернет. Для доступа к сервисам Oracle Cloud Service используется стандартный для отрасли протокол TLS. Подключения TLS формируются с использованием 128-разрядного или более надежного шифрования. Закрытый ключ, используемый для создания ключа шифрования, должен иметь длину не менее 2048 бит. TLS можно применять и настраивать для любых веб-приложений с сертификацией TLS. Для подключения к веб-программам рекомендуется использовать последние версии браузеров, поддерживающих шифрование высокой стойкости и улучшенные функции безопасности. Список сертифицированных браузеров для всех версий программ Oracle см. на портале поддержки Oracle для конкретного заказанного сервиса (например, на портале My Oracle Support). В отдельных случаях в облачных сервисах задействованы сторонние сайты, которые не контролируются корпорацией Oracle и используют нешифрованное подключение. Кроме того, иногда сторонние сайты, которые заказчик хочет интегрировать в облачный сервис, не принимают зашифрованные подключения. Если незашифрованное подключение к сторонним сайтам разрешено Oracle, по возможности мы будем использовать такие подключения наряду с зашифрованными.

Заказчики также могут получать доступ к сервисам Oracle Cloud посредством SSH или сервиса VPN с туннелем IPsec.

4.8. Повышение надежности и мониторинг системы

Oracle использует стандартные практики для повышения надежности систем Oracle Cloud, чтобы защитить их от потенциальных атак. Методы для повышения надежности платформы включают в себя ограничение доступа с помощью протоколов, удаление или отключение неиспользуемых сервисов и программ, удаление неиспользуемых учетных записей пользователя, управление обновлениями, журналирование и рассылку оповещений.

4.9. Ответные меры в случае инцидента безопасности

Oracle выполняет оценку рисков и принимает меры при подозрении несанкционированного доступа или действий в отношении данных заказчика, независимо от того, хранятся эти данные на оборудовании Oracle или на личных устройствах сотрудников и подрядчиков Oracle.

Наши операторы отслеживают и устраняют инциденты безопасности 24 часа в сутки, 365 дней в году. При получении уведомления, в зависимости от типа инцидента, организация Oracle Global Information Security (ГИБ) определяет порядок решения проблемы и назначает команды реагирования для ее устранения. При необходимости ГИБ ведет сотрудничество с заказчиками, техническими специалистами и органами безопасности. Целью группы реагирования является восстановление конфиденциальности, целостности и доступности клиентской среды, а также выявление и устранение причин инцидента. Сотрудники используют задокументированные процедуры для выявления и устранения потенциальных инцидентов несанкционированного использования данных, включая оперативную подготовку отчетности, порядок решения проблемы и методы охраны доказательств.

4.10. Предотвращение заражения вредоносным ПО

Вредоносное ПО может привести к нарушению конфиденциальности клиентских данных и их краже. Группа эксплуатации Oracle Cloud использует широкий набор методов по предотвращению, отслеживанию и устранению вредоносного ПО. На системах, используемых сервисами Oracle Cloud Services, устанавливается антивирусное и антивредоносное обеспечение. Распознанные вирусы и вредоносное ПО автоматические удаляются или помещаются в карантин. Определения вирусов и вредоносного ПО регулярно обновляются, и все доступные клиентские системы настроены для выполнения обновлений и сканирования в реальном времени. Организация Oracle Global Desktop Strategy (GDS) регулярно обновляет определения и устанавливает обновления безопасности для антивирусных/антивредоносных программ и серверов сервиса Windows Server Update Service (WSUS). GDS также может рассылать уведомления пользователям об угрозах и выходе обновлений безопасности для WSUS.

4.11. Внутренний надзор, осуществляемый руководством компании

Комитет Oracle по надзору за безопасностью (OSOC), состоящий из руководителей Oracle высшего звена, рассматривает и утверждает политики и программы Oracle в отношении безопасности и конфиденциальности. ГИБ — корпоративная организация, ответственная за надзор за безопасностью и применение политик на корпоративном уровне. Она также несет ответственность за разработку политик и стратегий для информационной безопасности и их применение, оценку безопасности информации и обучение. ГИБ выступает как основной контакт в случае инцидентов безопасности и обеспечивает координацию действий по их предотвращению, выявлению, расследованию и устранению.

Руководитель сервиса Oracle по обеспечению конфиденциальности информации осуществляет надзор и занимается решением проблем, связанных с соблюдением конфиденциальности. Организация Oracle Business Audit and Assessment отвечает перед советом директоров Oracle за проверку соответствия всех этих подразделений, а также за предоставление отчетов по результатам проверок.

4.12. Утилизация данных

По окончании предоставления услуг либо по запросу заказчика Oracle удалит среды или данные таким образом, чтобы устранить возможность доступа к ним или их чтения, за исключением случаев, когда закон запрещает удалять среду или данные частично или полностью.

4.13. Доставка физических носителей

Подготовкой физических носителей к отправке занимаются специально назначенные сотрудники Oracle в строгом соответствии с установленными процедурами. Цифровые носители вносятся в журнал, проходят процедуру шифрования и доставляются с соблюдением мер безопасности, и резервное копирование с последующим архивированием в хранилище выполняется сторонним поставщиком. Поставщики по договору обязуются соблюдать требования Oracle к защите носителей.

4.14. Конфиденциальность данных

Соглашение Oracle об обработке данных для сервисов Oracle Cloud и Политика конфиденциальности Oracle содержат сведения о порядке обработки данных, хранящихся в системах Oracle (включая персональные данные), к которым Oracle может получать доступ в связи с оказанием основных услуг. В соглашении об обработке данных подробно описаны роли Oracle и заказчика при обработке предоставляемых в рамках пользования сервисами персональных данных и управлении ими.

Эти документы доступны по следующим адресам:

» Соглашение об обработке данных для сервисов Oracle Cloud Services
http://www.oracle.com/dataprocessingagreement
» Политика конфиденциальности услуг Oracle
http://www.oracle.com/us/legal/privacy/services-privacy-policy-078833.html

4.15. Отчеты о результатах аудита, выполняемого сторонними организациями

Отчеты о результатах аудита сервисов Oracle Cloud Services периодически публикуются независимыми аудиторами (отчеты могут быть доступны не для всех сервисов и не в любое время). Заказчики могут запросить экземпляр актуального отчета о результатах аудита для нужного сервиса Oracle Cloud. Такие отчеты являются конфиденциальными, могут использоваться только заказчиками для оценки структуры и эффективности средств управления, применяемых в сервисах Oracle Cloud Services, и предоставляются по принципу «как есть» без каких-либо гарантий.

5. Единое управление идентификаторами и доступом

В Oracle Cloud применяется единое решение для управления идентификаторами и доступом, которое используется всеми типами сервисов Oracle Cloud, включая PaaS и IaaS. Идентификация является ключевой технологией, на основе которой заказчики Oracle получают безопасный доступ к сервисам PaaS и IaaS. Особенность Oracle Cloud, которая безопасно объединяет пользователей, сервисы и приложения, — это общие идентификаторы.

5.1. Именные домены арендаторов, пользователи и роли

Арендатор Oracle Cloud представляет собой заказчика, который оформил подписку на один или несколько сервисов Oracle Cloud. Обычно между арендатором Oracle Cloud и заказчиком Oracle существует однозначное соответствие. Именной домен в Oracle Cloud представляет собой пространство имен, выделенное арендатору. Именной домен используется для идентификации и связывания ресурсов арендатора и последующей изоляции информационных активов и операций одного арендатора от ресурсов и операций другого. Активы арендатора включают в себя сервисы и данные, в том числе такие артефакты безопасности, как пользователи, группы, токены, файлы cookies и политики. Заказчик Oracle может быть связан более чем с одним именным доменом Oracle Cloud.

Решение Oracle для управления идентификационными данными в облаке позволяет проводить аутентификацию и авторизацию пользователей, контролируя доступ к сервисам Oracle Cloud и функциям внутри них. Сервисная учетная запись Oracle Cloud — это уникальная учетная запись заказчика, с которой могут быть связаны облачные сервисы различных типов. Например, вы можете использовать три разных сервиса (Java, Database и IaaS) под одной учетной записью Oracle Cloud. Каждый сервис Oracle Cloud связан с именным доменом. С одним именным доменом могут быть связаны несколько сервисов с общими определениями пользователей и процедурами аутентификации. Пользователям домена могут быть предоставлены различные уровни доступа к каждому из связанных с доменом сервисов. При подписке на сервис Oracle Cloud для вас создается отдельный именной домен. Когда ваши пользователи входят в сервис Oracle Cloud с использованием сервисных учетных записей, средства управления идентификационными данными выполняют аутентификацию и определяют, какие возможности будут им доступны.

Возможности по управлению доступом в именном домене зависят от пользователей и их ролей. Пользователи с ролью администратора могут управлять локальными идентификаторами в облаке и их правами.

В именном домене можно управлять двумя типами пользователей.

- **Обычные пользователи.** Добавление учетных записей, пакетный импорт учетных записей, назначение ролей пользователям, изменение учетных записей, сброс паролей и удаление учетных записей.

» **Пользователи SFTP.** Установка паролей для учетных записей с защищенным FTP (SFTP). Учетные записи SFTP используются для входа на сервер SFTP для выполнения операций FTP, связанных с предоставлением сервисов Oracle Cloud.

В именном домене можно управлять двумя типами ролей.

» **Предопределенные роли.** Просмотр списка всех предопределенных ролей, созданных Oracle Cloud, и сопоставление его со списком пользователей, которым назначена выбранная роль.

» **Настраиваемые роли.** Просмотр, добавление и удаление роли, созданных для настраиваемого доступа к сервисам Oracle Cloud.

При активации сервисной учетной записи арендатора Oracle Cloud автоматически назначает заказчику следующие роли.

» **Администратор учетной записи.** Это — роль администратора сервисной учетной записи арендатора на уровне экземпляра сервиса. Она предоставляет пользователю привилегии по управлению одним или несколькими сервисами Oracle Cloud. Администратор учетной записи производит управление учетной записью арендатора Oracle Cloud посредством пользовательского интерфейса. Администратор учетной записи имеет привилегии по бизнес-надзору за экземплярами сервисов в одном или нескольких именных доменах. Администратор учетной записи может назначать администраторов сервисов и именных доменов для приобретенных им сервисов. Администратор учетной записи может просматривать показатели отдельных экземпляров сервиса.

» **Администратор именного домена.** Администратор именного домена управляет пользователями и их ролями. Администратор именного домена может просматривать только сведения о пользователях и ролях в закрепленном за ним именном домене. Администратор именного домена видит все роли на уровне домена и сервиса. Администратор именного домена является суперадминистратором для именного домена и всех входящих в него сервисов. Администратор именного домена может делегировать полномочия другим администраторам именного домена, а также управлять ролями, закрепленными за администратором сервиса. Администраторы именного домена могут выполнять обязанности администратора для всего именного домена.

» **Администратор сервиса.** Администратор сервиса является суперадминистратором для определенного экземпляра сервиса. Администратор сервиса может назначать на роль дополнительных администраторов сервиса, а также управлять другими ролями, связанными с сервисом. Тем не менее администраторы сервиса не могут создавать пользователей или роли.

5.2. Пароли

Пароли требуются для получения доступа ко всем учетным записям пользователей. Пароль указывается при создании учетной записи, и его можно изменить в любое время посредством

пользовательского интерфейса. Управление политиками паролей в Oracle Cloud осуществляется с помощью именного домена. Политика паролей — это набор правил для повышения компьютерной безопасности за счет надлежащего использования надежных паролей. Политики паролей часто являются частью корпоративных норм безопасности. Например, при смене пароля следует убедиться, что он соответствует требованиям политики паролей.

5.3. Единый вход с помощью SAML 2.0

Вы можете объединить корпоративное хранилище идентификаторов и именной домен, чтобы обеспечить единый вход (SSO) между локальными системами и сервисами Oracle Cloud. Единый вход позволяет пользователям получать доступ к нескольким доменам, введя учетные данные только на одном из них. Для обеспечения доступа через веб-браузер с возможностью единого входа Oracle Cloud использует стандартный язык обмена данными безопасности SAML 2.0. Единый вход позволяет предоставлять пользователям, прошедшим проверку подлинности в одном домене или локальном хранилище идентификаторов, доступ к другому домену. Например, вы можете организовать доступ пользователей к облаку посредством локального каталога, такого как Active Directory или Oracle Unified Directory. В основе единого входа лежит возможность объединения инфраструктуры идентификаторов. Сервис SSO использует язык SAML 2.0 для обмена сведениями между поставщиком учетных данных и поставщиком услуг.

Идентификационные данные в инфраструктуре Oracle Cloud хранятся в схемах LDAP. Как и большинство систем управления учетными данными, Oracle Cloud располагает хранилищем идентификаторов. Формат и правила для определения пользователей, групп и ролей определяются соответствующими схемами каталога LDAP.

5.4. Управление входом в сервис

Контингент пользователей в именном домене может быть разбит на следующие категории.

- **Неинтегрированные.** Хранятся в локальной системе управления идентификационными данными. Неинтегрированные учетные данные связаны только с Oracle Cloud. Как следствие, они известны только Oracle Cloud.
- **Интегрированные.** Хранятся в нескольких различных системах управления идентификационными данными и происходят из разных доменов. Идентификаторы интегрированным пользователям присваивает администратор. Эти идентификаторы передаются в Oracle Cloud посредством экспорта LDAP в сервис Oracle Shared Identity Management (SIM). Тем не менее такие пользователи не могут напрямую выполнить вход в сервис Oracle Cloud. Вместо этого их перенаправляют на сайт интегрированного (федеративного) сервиса для ввода учетных данных. Таким образом сервис единого входа Oracle Cloud получает подтверждение SAML от поставщика идентификаторов со сведениями о пользователе. Сервис единого входа Oracle Cloud разбирает подтверждение SAML и передает идентификатор именному домену.

5.5. Получение роли администратора

Получить роль администратора в Oracle Cloud очень просто. При регистрации учетной записи арендатора Oracle Cloud вам высылается электронное сообщение. Получив его, вы активируете учетную запись и выполняете вход в соответствующий сервис. Отправьте запрос для получения пробной подписки на веб-сайте Oracle Cloud. При этом система автоматически назначает вам следующие роли:

- Администратор учетной записи арендатора в Oracle Cloud.
- Администратор именного домена в именном домене.
- Администратор сервиса в сервисе.

Подробные сведения о концепции идентификаторов Oracle Cloud см. по адресу http://www.oracle.com/webfolder/technetwork/tutorials/obe/cloud/sharedidm/doc/Identity_Concepts.pdf

6. Меры обеспечения безопасности для конкретных сервисов

В следующих разделах рассказывается о способах обеспечения безопасности в сервисах Oracle Compute Cloud Service, Oracle Storage Cloud Service, Oracle Network Cloud Service, Oracle Database Cloud Service и Oracle Java Cloud Service.

6.1. Безопасность сервиса Oracle Compute Cloud Service

Изолирование экземпляра

Сервис Oracle Compute Cloud позволяет создавать и запускать виртуальные машины в инфраструктуре Oracle Cloud. Oracle Compute Cloud Service обеспечивает масштабируемые вычислительные мощности посредством экземпляров серверов в центрах обработки данных Oracle.

Безопасность сервиса Oracle Compute Cloud Service обеспечивается на нескольких уровнях: гипервизор, гостевая операционная система, динамический брандмауэр, вызовы API на основе маркеров, полномочия пользователей и защищенный доступ к экземплярам на основе SSH. Цель — предотвратить доступ к рабочим нагрузкам и данным заказчика со стороны несанкционированных пользователей или систем.

Как и в других облачных вычислительных системах, в основе Oracle Compute Cloud Service лежит виртуализация. Большинство претензий к безопасности виртуализации являются необоснованными. Риски виртуализации можно устранить с помощью различных аппаратных и программных изолирующих решений.

Первоочередным способом является изоляция инструкций ЦП. Intel VT-x и AMD-V создают монитор виртуальной машины, чтобы передать ей ресурсы ЦП для прямого использования. Машина может использовать их до тех пор, пока не попытается выполнить инструкцию ЦП, требующую особых полномочий доступа. На этом этапе работа виртуальной машины приостанавливается и ЦП возвращается монитору виртуальной машины.

Помимо изоляции инструкций ЦП, гипервизор обеспечивает изоляцию памяти и устройств за счет виртуализации физической памяти и физических устройств, в том числе дисков. Подобная разграниченная виртуализация физических ресурсов обеспечивает четкое разделение между гостевой операционной системой и гипервизором, обеспечивая безопасность вычислительной среды. Таким образом, экземпляры разных заказчиков, запускаемые на одной физической машине, изолированы друг от друга с помощью гипервизора.

В мультиарендном сервисе Oracle для эластичных вычислений логическая изоляция арендаторов осуществляется за счет виртуализации, как описано выше. Oracle также предлагает выделенное решение, представляющее собой полностью изолированный сервис для эластичных вычислений. Оно включает в себя выделенные физические серверы и ядра, а также сеть в ЦОД Oracle. Таким образом достигается полная изоляция операций ввода-вывода, ресурсов ЦП и сети. Сервис для выделенных вычислений использует ту же технологию виртуализации, которая используется для эластичных вычислений.

Сервис эластичных вычислений также позволяет разделить пространства имен API, гарантируя, что ресурсы не будут использованы не по назначению другими учетными записями.

Гостевая операционная система

Вы имеете полный административный доступ и права root для своих экземпляров. Oracle не имеет доступа к данным заказчика в экземплярах заказчика. Oracle поддерживает использование SSH, чтобы обеспечить безопасный вход в экземпляры Oracle Linux для вас и ваших пользователей. Oracle рекомендует создавать уникальные пары ключей SSH для каждого пользователя. Эти ключи не следует передавать Oracle или другим организациям.

Вы также несете ответственность за установку обновлений и исправлений для гостевой ОС, включая обновления безопасности. Предоставляемые Oracle образы машин Oracle Linux регулярно обновляются до последней версии.

Безопасный доступ к экземплярам с помощью SSH

Oracle поддерживает использование сетевого протокола SSH, чтобы обеспечить безопасный вход в экземпляры Oracle Linux для вас и ваших пользователей. Если используемый вами экземпляр создан с помощью предоставленного Oracle образа Oracle Linux, вы можете войти в этот экземпляр с помощью SSH как пользователь `opc`, который является пользователем по умолчанию для таких экземпляров.

Перед созданием вычислительного экземпляра следует создать по меньшей мере одну пару ключей SSH и загрузить открытый ключ SSH. Открытый ключ SSH можно отключить, включить и удалить. После входа в экземпляр в него можно добавить пользователей. Для этого необходимо создать еще одну пару ключей SSH для каждого пользователя, выполнить вход в экземпляр и назначить себя пользователем root. Затем вы можете создать нового пользователя и добавить для него открытый ключ SSH.

Динамический брандмауэр

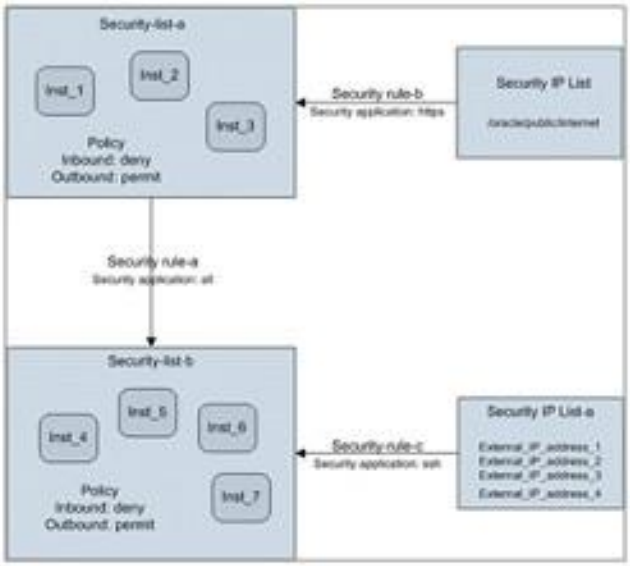
Oracle Compute Cloud Service предоставляет полное решение для контроля сетевого трафика в принадлежащих вам экземплярах с помощью брандмауэра. По умолчанию для брандмауэра установлен режим «отклонять все». Это означает, что при создании экземпляра он по умолчанию не пропускает сетевой трафик из других экземпляров и внешних узлов и в них. Вы можете полностью настраивать параметры доступа к принадлежащим вам экземплярам Oracle Compute Cloud Service как из других экземпляров, так и из внешних узлов. Можно настроить брандмауэр для групп и применять различные правила для различных классов экземпляров.

Чтобы обеспечить беспрепятственный обмен данными между несколькими экземплярами (например, чтобы все экземпляры, в которых размещена среда разработки, могли взаимодействовать друг с другом), можно создать список безопасности и добавить в него экземпляры. Экземпляр, добавленный в список, может взаимодействовать с другими экземплярами из этого списка. По умолчанию экземпляры в списке изолированы от узлов, не включенных в него. Это правило по умолчанию можно переопределить, создав правила безопасности. Все правила безопасности содержат конкретный источник, место назначения и комбинацию «протокол-порт», между которыми разрешена связь. Правила безопасности по сути представляют собой правила брандмауэра, которые можно использовать для организации трафика между экземплярами Oracle Compute Cloud Service из разных списков безопасности, а также между экземплярами и внешними серверами. Источник и место назначения в правиле безопасности могут представлять собой список безопасности IP-адресов (то есть список внешних серверов) или список безопасности. Приложение безопасности — это сопоставление «протокол-порт», которое можно использовать в правилах безопасности. Приложение безопасности можно создать, указав тип порта и порт, или использовать предопределенные приложения (такие как SSH, HTTPS, SNMP-TCP) в правилах безопасности. Например, вы можете создать правило, разрешающее доступ SSH через порт 22 с нескольких внешних серверов (перечисленных в списке безопасности IP-адресов), ко всем экземплярам в списке безопасности.

При создании экземпляра с помощью веб-консоли вы можете разрешить в настройках доступ для серверов в Интернете с помощью SSH. При выборе этого параметра созданный экземпляр добавляется в список безопасности по умолчанию и создается правило безопасности `DefaultPublicSSHAccess`, разрешающее доступ с помощью SSH к экземплярам в таком списке. Если доступ с помощью SSH не был разрешен при создании экземпляра, это всегда можно сделать позже. Для этого нужно создать список безопасности, добавить в него соответствующий экземпляр и применить правило безопасности. На приведенной ниже диаграмме показаны пути связи.

» Экземпляры из списка безопасности **a** могут отправлять трафик в экземпляры из списка безопасности **b** по любому протоколу в соответствии с правилом безопасности **a**.

» Экземпляры из списка безопасности **a** могут получать трафик HTTPS с любого сервера в сети Интернет в соответствии с правилом безопасности **b**.
» Экземпляры из списка безопасности **b** могут получать трафик с помощью SSH от любого из IP-адресов, включенных в список безопасности IP-адресов **a** в соответствии с правилом безопасности **c**.



Если правила безопасности для списка безопасности не определены, экземпляры из этого списка не могут получать трафик от серверов, не внесенных в этот список. Тем не менее экземпляры из списка по-прежнему могут получать доступ к экземплярам из этого же списка. При удалении экземпляра из списка безопасности этот экземпляр больше не может связываться с другими экземплярами в списке, а правила безопасности этого списка больше не влияют на движение трафика через экземпляр. Список безопасности IP-адресов содержит набор IP-адресов, которые служат в качестве источника правил безопасности. Список безопасности IP-адресов или список безопасности можно использовать в нескольких правилах безопасности. В случае конфликта политик преимущество имеет наиболее запретительная политика.

Вы можете подключать экземпляры к Интернету и получать доступ к ресурсам Oracle Cloud из любой точки благодаря зарезервированным IP-адресам.

Доступ с помощью API

Oracle Compute Cloud Service предоставляет интерфейс прикладного программирования REST, который можно использовать для программной подготовки и управления экземплярами и связанными ресурсами. Вызовы Oracle Compute Cloud Service с помощью API можно

осуществлять с использованием базовой аутентификации (имя пользователя и пароль) или проверки подлинности на основе токенов. Если запрос аутентификации выполнен успешно, сервер возвращает файл cookie, который содержит токен, действительный в течение 30 минут. Заказчик, совершающий вызовы с помощью API, должен включать в вызовы этот файл cookie. Время действия маркера аутентификации можно продлить на пять минут, выполнив команду `refresh_token`. Обновление маркера позволяет продлить сессию, но не более чем на время продолжительности сессии, равное трем часам.

Пользователи и роли

Страницу «Пользователи» на портале MyServices можно использовать для управления администраторами именного домена, администраторами сервисов, пользователями, ролями и паролями. (См. раздел «Единое управление идентификаторами и доступом».)

Для Oracle Compute Cloud Service можно использовать следующие предопределенные роли.

- **TenantAdminGroup (администратор именного домена)**. Пользователи, которым назначена эта роль, могут выполнять любые задачи в приложении MyServices, включая управление ролями и пользователями.
- **Service-instance-name.Compute_Operations (администратор сервиса)**. Пользователи, которым назначена эта роль, могут просматривать, создавать, обновлять и удалять ресурсы Oracle Compute Cloud Service. Администраторы именного домена при необходимости могут создавать дополнительных администраторов сервисов на портале Oracle Cloud MyServices. Чтобы обеспечить непрерывность деятельности, рекомендуется назначить по меньшей мере двоих пользователей с ролью Compute_Operations. Эти пользователи должны являться системными администраторами в вашей организации.
- **Service-instance-name.Compute_Monitor**. Пользователи, которым назначена эта роль, могут просматривать ресурсы Oracle Compute Cloud Service. Администраторы именного домена при необходимости могут создавать дополнительных пользователей с этой ролью на портале Oracle Cloud MyServices.

Безопасность блочной системы хранения

Система хранения представляет собой виртуальный диск, который предоставляет экземплярам постоянное, разделенное на блоки пространство для хранения данных. Oracle Compute Cloud Service позволяет создавать разделы хранения размером от 1 ГБ до 2 ТБ. За каждым экземпляром Oracle Compute Cloud Service можно закрепить 10 разделов хранения. Каждый раздел хранения можно закрепить только за одним экземпляром. Вы можете присоединить один или несколько разделов хранения за экземпляром либо при его создании, либо позже во время работы. После создания экземпляра не составляет труда увеличивать или уменьшать объем блочной системы хранения, присоединяя и отсоединяя разделы хранения. Однако разделы хранения, прикрепленные во время создания экземпляра,

отсоединить нельзя. Обратите внимание, что при отключении раздела хранения от экземпляра или удалении экземпляра данные в системе хранения сохраняются.

Доступ к разделу хранения разрешен только владельцу учетной записи Oracle Cloud, с использованием которой создавался раздел, и пользователям Oracle Cloud, имеющим разрешение на просмотр раздела и получение доступа к нему. Предоставление доступа таким пользователям осуществляется с помощью ролей, созданных в сервисе Oracle Shared Identity Management. (См. раздел «Единое управление идентификаторами и доступом»). Сервису Oracle Compute Cloud Service необходимы роли для выполнения следующих операций с разделом хранения:

- Создание и прикрепление раздела хранения. Создавайте разделы хранения и прикрепляйте их к экземплярам, чтобы обеспечить необходимый объем хранения для данных и приложений. Также можно связывать разделы хранения с образом машины, чтобы впоследствии использовать раздел хранения как загрузочный диск для экземпляра. Для выполнения этой операции пользователю должна быть назначена роль Compute_Operations.
- Удаление сведений о разделе хранения. Сведения о разделе хранения, такие как состояние, размер и экземпляр, к которому прикреплен раздел, можно просматривать с помощью веб-консоли. Для выполнения этой операции пользователю должна быть назначена роль Compute_Monitor или Compute_Operations.
- Удаление раздела хранения. При удалении раздела хранения все хранящиеся в нем данные и приложения будут удалены. Удалять раздел хранения следует, только если не планируется больше использовать хранящиеся в нем данные. Для выполнения этой операции пользователю должна быть назначена роль Compute_Operations.

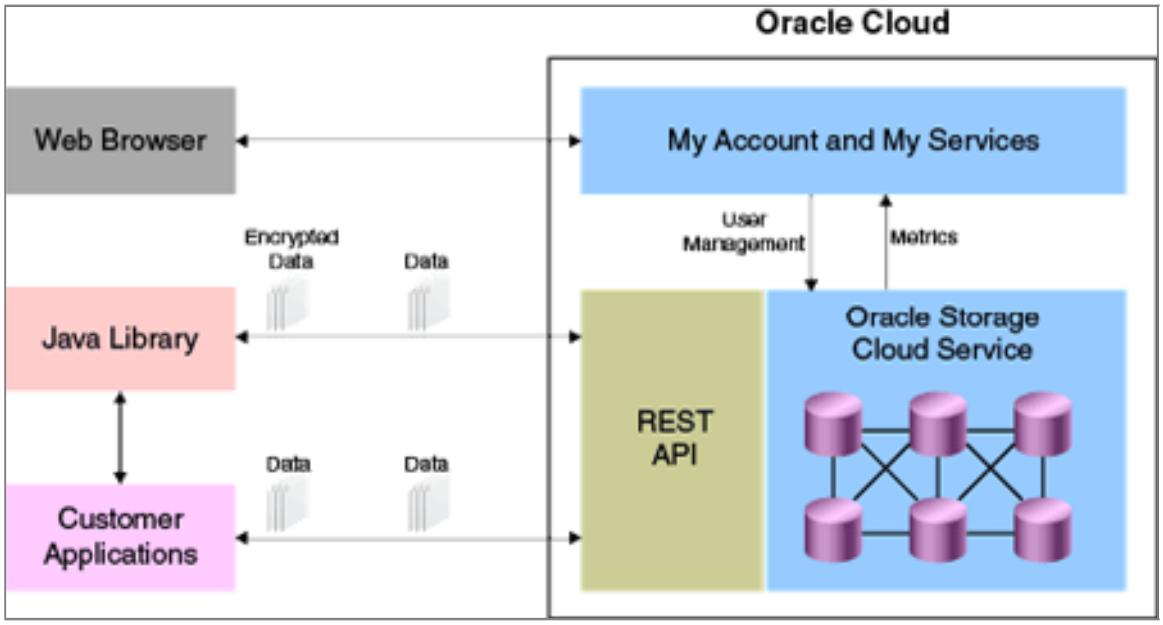
Шифрование дисков с конфиденциальной информацией помогает поддерживать безопасность. Для шифрования данных на виртуальных машинах можно использовать любые сторонние решения шифрования. Большинство решений предлагают возможности по управлению ключами, которые можно использовать для внедрения основной политики управления ключами.

6.2. Безопасность сервиса Oracle Storage Cloud Service

Oracle Storage Cloud Service — продукт типа «инфраструктура как услуга» (IaaS), представляющий собой многоуровневое решение корпоративного класса для хранения неструктурированных данных и получения к ним доступа в любое время с любого устройства. Оно идеально подходит для резервного копирования данных, архивации, совместной работы с файлами, а также для хранения больших объемов неструктурированных данных, таких как журналы, данные от датчиков и образы виртуальных машин.

Архитектура Oracle Storage Cloud Service отличается высокой доступностью и устойчивостью. Прямой доступ к ней можно получить посредством REST API, непрямой — посредством NFSv4, клиентских SDK и сторонних приложений. При хранении объектов в Oracle Storage Cloud Service данные тиражируются по нескольким узлам ЦОД. Эта стратегия обеспечивает сохранность данных объекта в случае выхода из строя оборудования.

На приведенной ниже диаграмме представлен обзор архитектуры Oracle Cloud Storage Service.



Доступ для чтения и записи объектов

Oracle Storage Cloud Service хранит данные как объекты в контейнерах с горизонтальной иерархией. Объекты обычно создаются путем загрузки файлов. Также они могут создаваться на основе неструктурированных динамических данных. Объекты создаются в контейнере. Один объект может вмещать до 5 ГБ данных, а для размещения свыше 5 ГБ несвязанных данных требуется объединить несколько объектов. Контейнер — созданный пользователем ресурс, в котором может быть размещено неограниченное число объектов, если не установлено пороговое значение. Контейнеры нельзя вкладывать друг в друга.

Доступ к объекту для чтения и записи данных регулируется с помощью списков контроля доступа для контейнера, в котором находится объект. Каждому контейнеру можно назначить собственные списки. По умолчанию контейнер и объекты в нем являются частными, т. е. доступны только пользователю, создавшему контейнер, однако при желании можно предоставить право доступа для чтения другим пользователям.

Пользователи, которым назначена роль администратора системы хранения, по умолчанию имеют права на чтение и запись для всех контейнеров в своем экземпляре сервиса. В отношении пользователей, не являющихся администраторами, действуют правила, назначенные для конкретного контейнера. Исключением является путь к корневому каталогу экземпляра, так как ему нельзя назначить список контроля доступа. Все пользователи могут видеть список контейнеров в этом пути, однако создавать или удалять контейнеры могут только администраторы системы хранения.

Доступ с помощью API

Основным способом получения доступа к Oracle Storage Cloud Service являются веб-сервисы RESTful на основе OpenStack Swift. Доступ к сервису можно получить через Интернет в любое время, из любой точки и с любого устройства. Также доступна библиотека Java, включающая в себя веб-сервис RESTful. Для пользования сервисом не требуется специальное оборудование.

Пользователи и роли

Страницу «Пользователи» на портале MyServices можно использовать для управления администраторами именного домена, администраторами сервисов, пользователями, ролями и паролями. (См. раздел «Единое управление идентификаторами и доступом».)

Для сервиса Oracle Storage Cloud Service можно использовать следующие предопределенные роли.

- **TenantAdminGroup (администратор именного домена)**. Пользователи, которым назначена эта роль, могут выполнять любые задачи в приложении MyServices, включая управление ролями и пользователями.
- **Storage.Storage_Administrator (администратор сервиса)**. Пользователи, которым назначена эта роль, могут выполнять любые задачи в экземпляре Oracle Storage Cloud Service, в том числе управлять пользователями. Такие пользователи могут также отслеживать работу сервисов и управлять ими, назначать пользователям роли, создавать и удалять контейнеры и изменять списки контроля доступа к ним. Для неизмеряемых подписок имя роли будет выглядеть следующим образом: имя-экземпляра-сервиса.Storage_Administrator.
- **Storage.Storage_ReadWriteGroup**. Пользователи, которым назначена эта роль, могут создавать, читать, изменять и удалять объекты в контейнерах, а также просматривать списки контейнеров и содержащихся в них объектов (если роль не была удалена из списка контроля доступа, дающего право чтения). Для неизмеряемых подписок имя роли будет выглядеть следующим образом: имя-экземпляра-сервиса.Storage_ReadWriteGroup.
- **Storage.Storage_ReadOnlyGroup**. Пользователи, которым назначена эта роль, могут читать объекты в контейнерах, а также просматривать списки контейнеров и содержащихся в них объектов (если роль не была удалена из списка контроля доступа, дающего право чтения). Для неизмеряемых подписок имя роли будет выглядеть следующим образом: имя-экземпляра-сервиса.Storage_ReadOnlyGroup.

Шифрование объектов

Прежде чем отправить объекты в Oracle Storage Cloud Service, их можно подвергнуть шифрованию. Для этого можно использовать библиотеку Java или любое другое шифровальное решение.

При использовании возможностей шифрования библиотеки Java на стороне заказчика все шифровальные процессы осуществляются в библиотеке за пределами сервиса. Шифрование может выполнить любой пользователь, которому назначена роль администратора или роль, входящая в список контроля доступа X-Container-Write.

При использовании библиотеки Java для всех объектов, создаваемых в Oracle Storage Cloud Service, создается уникальный симметричный ключ. Библиотека Java использует этот ключ для шифрования данных перед сохранением. Кроме того, администратор обязан создать асимметричную пару ключей и управлять этими ключами. После шифрования данных библиотека Java зашифровывает симметричный ключ конверта с помощью асимметричной пары. Обратите внимание на то, что ранее использовавшуюся пару ключей можно заменить на новую без необходимости загружать объект и выполнять повторное шифрование. Ключ конверта хранится в виде метаданных вместе с данными объекта.

При использовании библиотеки Java для получения доступа к таким зашифрованным объектам ключ конверта извлекается и расшифровывается с помощью симметричной пары ключей, предоставляемой заказчиком. Затем полученный симметричный ключ используется для расшифровки данных объекта. Поскольку ключ конверта представляет собой метаданные объекта, удаление и повреждение этого ключа ведет к утрате зашифрованных данных объекта. Чтобы избежать этого, рекомендуется ограничить возможности доступа с правом записи для зашифрованных объектов на стороне заказчика.

Обратите внимание, что к объектам, зашифрованным с помощью библиотеки Java, нельзя получить доступ с помощью REST API, поскольку Oracle Storage Cloud Service хранит ключ конверта в объекте в виде метаданных и Oracle не сообщает способа для извлечения и расшифровки ключа и последующей расшифровки объекта. Если объект зашифрован заказчиком с помощью библиотеки Java, для получения доступа к объекту следует использовать только ее. Зашифрованные этим образом объекты также нельзя расшифровать без помощи библиотеки Java.

Возможности шифрования библиотеки Java поддерживают только 2048-битовые пары ключей RSA, шифрование выполняется только для данных объекта, но не для его метаданных. Сегментированные объекты зашифровать нельзя. Незашифрованные объекты нельзя загрузить с использованием возможности шифрования.

Заказчики также могут использовать собственные решения для шифрования данных перед сохранением их в Oracle Storage Cloud Service. В этом случае для получения доступа к зашифрованным объектам следует использовать REST API.

Обратите внимание, что при использовании шифрования на своей стороне заказчик несет ответственность за управление всем жизненным циклом ключей шифрования, включая их создание, чередование и архивацию.

Безопасность Oracle Storage Cloud Software Appliance

Oracle Storage Cloud Software Appliance — виртуальная платформа, обеспечивающая простое, надежное и безопасное хранение и получение данных из сервиса Oracle Storage Cloud Service. Чтобы гарантировать защиту данных и при их хранении в Oracle Storage Cloud Service и при передаче, воспользуйтесь возможностями шифрования Oracle Storage Cloud Software Appliance, прежде чем отправить данные в сервис Oracle Storage Cloud Service.

Шифрование данных в Oracle Storage Cloud Software Appliance осуществляется с помощью симметричного ключа, который хранится в базе данных платформы и зашифрован с помощью асимметричной пары открытого и закрытого ключей. Администраторы могут выполнять резервное копирование и сохранять асимметричные ключи, чтобы использовать их для восстановления зашифрованных данных.

При сохранении файла в Oracle Storage Cloud Software Appliance он сохраняется в кэш локального диска в исходном виде. Шифрование выполняется перед загрузкой файла в Oracle Storage Cloud Service. При получении файла из Oracle Storage Cloud Service выполняется расшифровка файла с одновременным сохранением в кэш локального диска.

Чтобы включить шифрование файловой системы, следует установить флажок в поле «Включить шифрование» (Enable Encryption) при создании файловой системы на консоли управления. После этого можно создавать ключи шифрования и определять ключи на консоли управления. При необходимости ключи шифрования можно изменить.

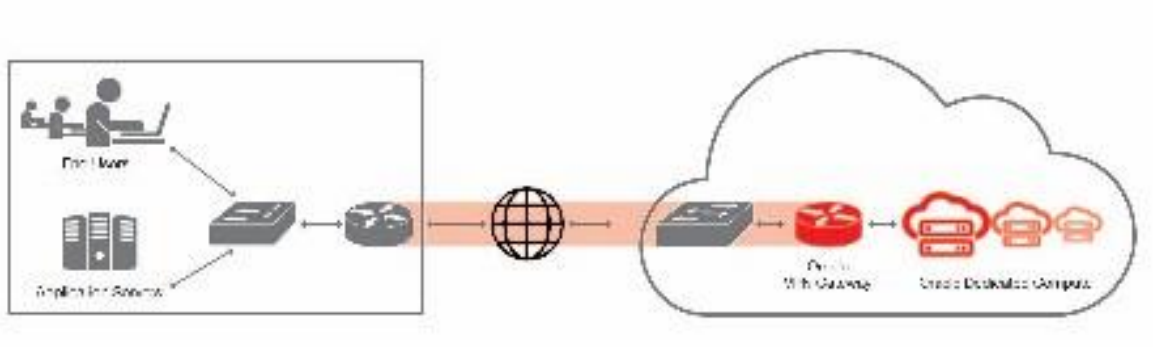
Шифрование на уровне контейнера позволяет зашифровать только конфиденциальные данные, что повышает эффективность хранения. Встроенные средства для проверки целостности данных гарантируют полную сохранность данных при их перемещении в любом направлении на всем пути назначения.

6.3. Безопасность сервиса Oracle Network Cloud Service

Oracle Cloud включает в себя ряд сетевых сервисов для создания логически изолированной сети, подключения к частной сети Oracle Cloud и определения предсказуемого маршрута с предсказуемой производительностью.

VPN типа «сеть-сеть» для выделенных вычислений

Oracle Cloud позволяет создавать безопасные подключения из клиентской зоны Oracle Compute Cloud Service, устанавливая защищенный туннель IPsec между VPN-шлюзом Oracle и шлюзом в клиентском ЦОД.



VPN типа «сеть-сеть» для выделенных вычислений предлагает следующие возможности:

- Создание нескольких туннелей между узлами в зоне Oracle Compute Cloud Service.
- Настройка диапазона IP-адресов для вычислительных экземпляров.
- Доступ экземпляров к другим облачным сервисам Oracle.
- Настройка внешнего IP-адреса для доступа через Интернет.
- Полное шифрование данных, перемещаемых между клиентским ЦОД и облачным сервисом выделенных вычислений Oracle с помощью 128-битного симметричного ключа шифрования AES.
- Организация VPN-устройств в кластер для обеспечения высокой доступности.

Oracle Cloud REST API поддерживает две модели VPN типа «сеть-сеть»:

- **Шлюз VPN**. Модель шлюза VPN представляет сетевое устройство, обеспечивающее функционал шлюза VPN. Шлюз содержит сведения для получения доступа к устройству, такие как IP-адрес, учетные данные и имена интерфейсов, связанных с зоной Oracle Compute Cloud Service.
- **Конечные точки VPN**. Модель конечных точек VPN представляет собой конечную точку VPN, подключенную к другой точке на удаленном конце туннеля VPN. Конечная точка VPN создается на шлюзе VPN. Эта модель включает в себя такие атрибуты, как IP-адрес другой точки, общий ключ, доступные маршруты для этой точки и наличие подключения VPN.

Мультиарендная VPN на основе Corente Cloud Services Exchange

Oracle Network Cloud Service включает в себя мультиарендное решение на основе IPSec VPN, использующее распределенную виртуальную платформу на границах сети, которая автоматически устанавливается и обеспечивает безопасные конечные точки для виртуальных частных сетей поверх любых IP-сетей. Служебный шлюз устанавливается в ЦОД заказчика, обеспечивая безопасное сквозное подключение между ЦОД и Oracle Cloud.

FastConnect

Большинство корпоративных приложений очень чувствительны к колебаниям задержки и задержкам в целом. Когда приложениям в частном облаке (работающем по гибридной модели) требуется постоянный показатель задержки, стоит опасаться сбоев сети Интернет. FastConnect устраняет эту проблему, обеспечивая фиксированные показатели задержки. FastConnect обеспечивает частное подключение с высокой пропускной способностью между ЦОД заказчика и Oracle Cloud, стабилизируя производительность сети.

Передача больших объемов данных через Интернет — непредсказуемый процесс, что может вести к снижению производительности или задержкам при выполнении пакетных заданий. Рост требований к передаче данных растет, вынуждая компании увеличивать пропускную способность корпоративных сетей, что ведет к увеличению расходов, но не гарантирует окупаемости этих вложений или общего улучшения производительности. FastConnect решает эту проблему за счет переноса трафика Oracle Cloud на выделенный маршрут, что помогает улучшить производительность сети и снижает показатели задержки при дополнительном использовании возможностей размещения в ЦОД Equinix. Заказчики Oracle могут получить партнерскую редакцию FastConnect на Equinix Cloud Exchange.

Для этого на стороне заказчика необходимо выполнение следующих требований:

- Наличие сетевого оборудования с поддержкой маршрутизации на уровне 3 с помощью BGP, установленного на Equinix IBX в городе, где будет производиться обслуживание.
- Обеспечение возможности подключения к ECX-L3 в городе, где будет производиться обслуживание.
- Наличие действительного заказа Oracle на FastConnect Partner Edition с соответствующей скоростью передачи данных через порт (в настоящее время 1 или 10 Гбит/с).
- Наличие действующего IP-адреса и номера в автономной системе (ASN) для подключения к Equinix Cloud Exchange. Чтобы получить IP-адрес и номер ASN, свяжитесь со своим поставщиком услуг Интернета или одним из органов регистрации.

6.4. Безопасность сервиса Oracle Database Cloud Service

Oracle Database Cloud Service обеспечивает широкие возможности и гибкость облачной СУБД Oracle Database. Вы можете выбрать выделенный экземпляр базы данных с полным административным управлением или выделенную схему в БД, где все задачи по сопровождению платформы для разработки и развертыванию выполняются Oracle. В этом документе особое внимание уделяется возможностям обеспечения безопасности в экземпляре с полным административным управлением. Сервис «схема в БД» представляет собой полностью управляемое облачное решение и ограничивает возможности заказчика в том, что касается изменения настроек безопасности по умолчанию.

Oracle Database Cloud Service Enterprise Edition предоставляет предварительно настроенные выделенные виртуальные машины, позволяющие развертывать экземпляры СУБД Oracle Database 12c или Oracle Database 11g. Oracle Database Cloud Service предоставляет вычислительные образы на основе виртуальных машин (общего назначения и с расширенным объемом памяти), которые обеспечивают полные возможности СУБД Oracle Database для приложений всех видов, предназначенных как для рабочих нагрузок, так и для разработки и тестирования. Oracle Database Cloud Service идеально подходит для организаций, которым требуется полноценная облачная версия СУБД Oracle, но при этом сохраняется полный административный контроль, в том числе доступ с правами root к ОС и административный доступ к базе данных. Oracle Database Cloud Service обеспечивает современный облачный инструментарий для простого управления базами данных, включая автоматическое резервное копирование с возможностью восстановления на заданный момент времени и установку обновлений и исправлений одним щелчком мыши.

Доступ с помощью SSH

Для обеспечения безопасного доступа к порту на вычислительном узле заказчика, связанном с экземпляром Oracle Database Cloud Service, используется программное обеспечение Secure Shell (SSH) с поддержкой туннелирования. При создании экземпляра Oracle Database Cloud Service доступ по сети к вычислительным узлам предоставляется через подключения SSH к порту 22.

Некоторые клиенты SSH с поддержкой туннелирования предоставляются бесплатно. На платформе Linux можно использовать служебную программу `ssh`. Если доступ к экземпляру базы данных выполняется из ОС Windows, можно использовать PuTTY, бесплатный клиент SSH с поддержкой туннелирования. После создания туннеля SSH в Linux или Windows можно получить доступ к порту на целевом вычислительном узле с помощью команды `localhost:local-port`, где `local-port` — порт-источник, указанный при создании туннеля. В Mac OS клиент SSH установлен по умолчанию.

Безопасный доступ к экземплярам базы данных

Oracle Database Cloud Service использует сервис Oracle Compute Cloud Service для безопасного сетевого доступа к экземплярам баз данных в облаке. Консоль Oracle Compute Cloud Service может использоваться для операций сетевого доступа, таких как предоставление доступа к порту на вычислительном узле, связанном с базой данных в облаке.

Сетевое шифрование и обеспечение целостности данных в сети

Заказчики Oracle Database Cloud Service могут использовать возможности сетевого шифрования базы данных, чтобы обеспечить безопасность подключений к своим облачным базам данных. Протоколы SSL/TLS позволяют зашифровывать подключения баз данных по сети и при необходимости сконфигурировать для них взаимную аутентификацию. Нативное сетевое шифрование по внутреннему протоколу Oracle (SQLNet) позволяет использовать шифрование и при необходимости проводить проверку целостности данных, чтобы предотвратить изменение данных при передаче и несанкционированное воспроизведение. Эти функции поддерживают сложные стандарты сетевого шифрования, такие как Advanced Encryption Standard (AES). Функции для проверки целостности поддерживают современные алгоритмы хеширования, включая SHA-2.

По умолчанию экземпляры и клиенты баз данных Oracle Database Cloud Service настроены для выполнения нативного сетевого шифрования по внутреннему протоколу Oracle (SQLNet) и проверки целостности данных. Если отменить сетевое шифрование в настройках клиента базы данных, сервер интерпретирует это как потенциальную угрозу и в соответствии с настройками по умолчанию отклонит соединение.

Шифрование хранящихся данных

Создаваемые пользователями табличные пространства, в которых обычно хранятся данные заказчиков, по умолчанию подвергаются шифрованию в сервисе Oracle Database Cloud Service. Новые табличные пространства, создаваемые с помощью команды `SQL CREATE TABLESPACE` или использующих эту команду инструментов, по умолчанию зашифровываются с помощью алгоритма AES128. Некоторые стандартные табличные пространства, являющиеся частью внутренней системы базы данных, не шифруются. Шифрование данных в табличных пространствах доступно во всех стандартных и корпоративных редакциях и версиях Oracle Database Cloud Service Enterprise Edition.

Заказчики также могут шифровать резервные копии RMAN и экспортные файлы, созданные функцией Data Pump, в облачных базах данных. Оптимизации в базе данных проходят через предварительно зашифрованные данные в табличных пространствах, а при необходимости выполняется шифрование всего потока данных. Резервные копии и экспортированные файлы можно зашифровать с помощью того же ключа безопасности, который использовался для шифрования табличного пространства, с помощью пароля или их комбинации.

Мастер ключи, используемые для шифрования хранящихся данных, автоматически создаются базой данных и хранятся в личном бумажнике Oracle Wallet. Уполномоченный администратор безопасности клиентской базы данных может периодически заменять используемый ключ с помощью команд SQL. Использованные ключи хранятся в бумажнике Oracle Wallet, чтобы при необходимости восстанавливать зашифрованные резервные копии. Заказчикам, имеющим несколько баз данных с постоянно расширяющимися бумажниками, рекомендуется использовать Oracle Key Vault (отдельно лицензируемый продукт), чтобы обеспечить централизованное управление ключами шифрования и бумажниками. Oracle Key Vault — программная платформа с дополнительными возможностями защиты, которая устанавливается в корпоративном ЦОД и подключается к зашифрованным базам данных в Oracle Cloud или локальной системе.

Дополнительные средства для управления безопасностью

Oracle Database Cloud Service предлагает ряд дополнительных средств для обеспечения базовой безопасности важных данных в облаке. Эти средства доступны для всех баз данных и могут быть настроены после развертывания базы.

К основным средствам управления относятся права и роли пользователей. В соответствии с принципом безопасности, предписывающим ограничение прав, рекомендуется назначать пользователям облачной базы данных только необходимые права и роли. Другим базовым средством управления является аудит. Он используется для фиксации записей о действиях в базе данных и отслеживания вредоносных активностей. Чтобы применять аудит максимально эффективно, рекомендуется установить Oracle Audit Vault и Oracle Database Firewall (отдельно лицензируемые продукты). Это позволяет перенести сведения, связанные с аудитом, в центральное локальное хранилище и создавать в нем отчеты по действиям в базе данных и получать уведомления безопасности. Данные решения также включают в себя брандмауэр для базы данных и средства для мониторинга SQL-запросов, что позволяет отслеживать неавторизированные действия на ранних этапах и при необходимости блокировать угрозы до нанесения ущерба. Также для конкретных типов подписки и версий баз данных доступны дополнительные бесплатные средства безопасности, обеспечивающие профилактику. Их можно использовать для превентивного ограничения доступа к наиболее важным конфиденциальным или регулируемым сведениям в Oracle Database Cloud Service. Многие из этих средств уникальны и доступны только для баз данных Oracle.

Средство	Описание	Охват (подписки на облачные сервисы)				Доступность (версия базы данных)	
		Enterprise Edition	High Perf.	Extreme Perf.	Exadata Service	Oracle Database 12c	Oracle Database 11gR2
Advanced Security Data Redaction	Удаляет конфиденциальные данные из результатов поиска в облаке до отображения данных в приложении. Сокрытие данных производится без ущерба производительности и в соответствии с условиями политик.		Да	Да	Да	Да	Да
Database Vault	Снижает риск утечки конфиденциальных сведений через наделенных широкими полномочиями пользователей, таких как администраторы баз данных, и привилегированные подключения к приложениям. Ограничивает действия, доступные для таких приложений. Вводит ограничения исходя из условий и факторов выполнения.		Да	Да	Да	Да	Да
Label Security	Реализует разработанную Министерством обороны США концепцию многоуровневой безопасности (MLS), обеспечивая размещение в одной таблице строк разной степени конфиденциальности. Создает разметку для строк в облачных базах данных в соответствии с группой, категорией и уровнем конфиденциальности.		Да	Да	Да	Да	Да
Real Application Security	Предоставляет разработчикам приложений платформу для определения учетных записей в легковесных базах данных (без схем БД) и всесторонней авторизации объектов. Позволяет разработчикам авторизовать собственную модель безопасности на уровне СУБД Oracle Database и использовать эту модель в нескольких пользовательских приложениях.	Да	Да	Да	Да	Да	

Базы данных, запускаемые в Oracle Database Cloud Service, можно использовать в качестве источников данных для Oracle Data Masking and Subsetting Pack, дополнительного пакета для Oracle Enterprise Manager 12c. Это средство упрощает удаление конфиденциальных сведений из копий продуктивных данных в облачном сервисе, которые предназначены для бизнес-партнеров, не задействованных в производстве, например занимающихся разработкой и тестированием баз данных. Лицензия на источник данных для Oracle Data Masking and Subsetting Pack включена в подписки для High Performance, Extreme Performance и Exadata Service. Она может использоваться в СУБД Oracle Database 11g R2 или Oracle Database12c.

6.5. Безопасность сервиса Oracle Java Cloud Service

Oracle Java Cloud Service — это полнофункциональная платформа для создания и развертывания приложений Java EE и управления ими. Вы получаете лучший в отрасли сервер приложений, который запускается в облачной среде корпоративного класса. В основе платформы лежит

Oracle WebLogic Server, сервер приложений № 1 для традиционной и облачной среды. Также в вашу среду можно добавить кэширование с помощью Oracle Coherence и распределенную grid-среду доступа к данным.

Корпоративная среда предварительно устанавливается и настраивается с применением лучших практик Oracle для развертывания приложений, что позволяет максимально увеличить производительность, масштабируемость и надежность. Возможности обеспечения безопасности соответствуют предлагаемым в Oracle Cloud IaaS. Такие возможности, как эластичные вычисления и система хранения, позволяют выполнять любые рабочие нагрузки в Oracle Java Cloud Service и расширять среду по мере необходимости.

Безопасность всех приложений, развертываемых в экземпляре Oracle Java Cloud Service, обеспечивается так же, как в среде приложений, а управление безопасностью — как в локальном экземпляре Oracle WebLogic Server.

В настройках безопасности по умолчанию используются пользователи, группы, роли и политики безопасности, определенные в схемах по умолчанию для аутентификации, авторизации и учетных данных, а также в схемах ролей для поставщиков безопасности. По умолчанию проведена базовая настройка поставщиков безопасности для WebLogic Server, а встроенный сервер LDAP для WebLogic Server используется как хранилище данных для этих поставщиков.

Чтобы применить настройки безопасности по умолчанию к корпоративному экземпляру Oracle Java Cloud Service, используется консоль управления WebLogic Server. С ее помощью можно определять пользователей, группы и роли для области безопасности, а также создавать политики безопасности для защиты ресурсов WebLogic Server в домене.

Если настройки по умолчанию не соответствуют корпоративным требованиям, можно создать новую область безопасности с любым сочетанием поставщиков безопасности, как предлагаемых WebLogic Server, так и пользовательских. Затем новая область безопасности назначается областью по умолчанию. Вместо встроенного сервера LDAP Oracle рекомендует использовать для рабочих приложений систему управления идентификаторами, например Oracle Identity Management.

Пользователи и роли

Oracle Java Cloud Service использует роли для контроля доступа к задачам и ресурсам. При создании учетной записи Oracle Java Cloud Service администратору сервиса присваивается роль администратора Java, а также прочие служебные роли, необходимые для работы со связанными сервисами Oracle Cloud. Прежде чем кто-либо сможет получить доступ к Oracle Java Cloud Service, необходимо создать учетные записи для администратора Java и прочих служебных ролей. Только администратор именного домена может создавать учетные записи пользователей и назначать роли.

Пользователи, которым назначена роль администратора Java, могут выполнять в экземпляре сервиса различные действия, такие как создание, удаление, запуск, остановка, масштабирование, обновление, резервное копирование и восстановление. Также такие пользователи могут управлять балансировщиками нагрузки для экземпляров, отслеживать использование сервисов в Oracle Cloud и управлять ими.

Если сервис Oracle Coherence включен для данного экземпляра сервиса, администратор Java может добавить к нему или удалить из него уровень хранения данных Oracle Coherence (только REST API).

При создании экземпляра Oracle Java Cloud Service создаются следующие учетные записи администратора для виртуальной машины Oracle Compute Cloud Service и Oracle WebLogic Server:

- Пользователь ОС виртуальной машины, `opc`, имеет возможность доступа с правами root к операционной системе, установленной на виртуальной машине. Пользователь может подключиться к виртуальной машине посредством SSH и получить прямой доступ на уровне виртуальной машины к экземпляру Oracle Java Cloud Service. Пользователь `opc` может создавать на виртуальной машине другие учетные записи для работы с операционной системой с помощью интерфейса SSH. Учетные данные пользователя `oracle` нельзя использовать для входа в машину. Этот пользователь имеет только стандартные полномочия для запуска и прекращения работы продуктов Oracle, установленных на машине.
- Администратор WebLogic Server может управлять Oracle WebLogic Server в Oracle Java Cloud Service, а также получать доступ к консоли управления WebLogic Server и использовать ее. Администратор WebLogic также может управлять пользователями и группами в LDAP, а также настраивать других поставщиков идентификаторов.

Обратите внимание, что хранение учетных записей администратора WebLogic Server и пользователей ОС виртуальной машины, а также управление ими недоступно в Oracle Cloud. Имя пользователя и пароль для администратора WebLogic Server указываются при создании экземпляра Oracle Java Cloud Service. Хранение учетных данных и полномочий для администратора WebLogic Server и всех созданных им учетных записей, а также управление ими происходит в Oracle WebLogic Server. Дополнительные сведения об обеспечении безопасности экземпляров Oracle Java Cloud с помощью WebLogic Server см. в документах, размещенных на сайте Oracle.

7. Подход Oracle к разработке безопасных облачных сервисов

Разработка облачных сервисов Oracle ведется в соответствии с программой обеспечения безопасности программного обеспечения Oracle Software Security Assurance (OSSA). OSSA — совокупность методов, применяемых Oracle для обеспечения безопасности при проектировании, создании, тестировании и предоставлении услуг.

Безопасность учитывается на всех этапах разработки облачного сервиса, от начальной концепции архитектуры до обслуживания после выпуска продукта. Ниже приведен краткий обзор всех стадий разработки программного обеспечения в Oracle:

» Стадия проектирования. Обучение основным принципам безопасности и надежные стандарты кодирования, применяемые в Oracle, гарантируют, что инженеры, архитекторы и руководители проектов принимают оптимальные решения по обеспечению безопасности. Оценка угроз при анализе рисков архитектуры помогает выявить потенциальные проблемы на самых ранних стадиях разработки.
» Стадия написания кода. Мы устраняем стандартные виды уязвимостей за счет безопасных стандартов и шаблонов кодирования. На этой стадии мы используем инструменты для статического анализа кода, чтобы выявить проблемы безопасности, и устраняем все серьезные неполадки, прежде чем перейти к стадии тестирования.
» Стадия тестирования. Для выявления потенциальных проблем безопасности наши специалисты и независимые консультанты используют внутренние инструменты Oracle, инструменты сторонних разработчиков для динамического анализа и тестирования, а также ручные проверки.
» Перед запуском сервиса. Прежде чем выпустить продукт на рынок, мы выполняем проверку с целью убедиться, что разработанный функционал соответствует требованиям Oracle к безопасности облачных сервисов. Оценка и мониторинг продукта на потенциальные проблемы безопасности проводятся независимыми специалистами.

Подробные сведения о программе обеспечения безопасности программного обеспечения Oracle Software Security Assurance см. в документах на сайте.

8. Заключение

Защита данных заказчика является одним из основных вопросов при разработке всех типов инфраструктур и сервисов Oracle для публичного облака. Решения Oracle Cloud были разработаны с целью обеспечить безопасность для инфраструктур и платформ, используемых заказчиками Oracle для выполнения критически важных рабочих нагрузок и хранения данных. Мы полагаем, что обладаем правильными стратегией, философией, навыками и ресурсами безопасности для того, чтобы обеспечить защиту данных заказчиков и помочь заказчикам в создании безопасных и защищенных облачных решений. Мы продолжим работать над средствами обеспечения безопасности, чтобы и дальше создавать самые надежные публичные облачные инфраструктуры и проверенные облачные решения. Эти возможности позволяют заказчикам Oracle легко обеспечивать высокий уровень защиты, с уверенностью справляться с любыми рабочими нагрузками и создавать надежные гибридные облачные решения.

Россия 142784, **Москва,** пос. Московский, Киевское шоссе, 22 км, д. 6, стр.1, Бизнес-центр ComCity. Тел.: +7(495) 641-1400. Факс: +7(495) 641-1414

Россия 630099, **Новосибирск,** ул. Каменская, д.7, БЦ Хилтон, офис 305. Тел.: +7 (383) 291-00-85

Украина 01601, **Киев** ул. Мечникова 2, бизнес-центр «Парус»; 16-ый эт. Тел.: +380 (44) 490-90-50. Факс: +380 (44) 490-90-51

Казахстан 050051, **Алматы,** мкр. Самал 2/97, Бизнес Центр «Самал Тауэрс», 6 этаж, Блок А2. Тел.: +7(727) 320-11-80. Факс: +7 (727) 258-47-44

ORACLE

СВЯЖИТЕСЬ С НАМИ

blogs.oracle.com/russia

facebook.com/oracle.russia

twitter.com/oracleRU

oracle.com/ru

Integrated Cloud Applications & Platform Services

Семейство продуктов Oracle Database 12c
Автор: Дженни Гельхаузен (Jenny Gelhausen)
Соавторы: Пенни Эврил (Penny Avril), Уилли Харди (Willie Hardie)

Oracle is committed to developing practices and products that help protect the environment