Средства управления безопасностью
Oracle Gen 2 Exadata Cloud@Customer

ORACLE

Средства управления безопасностью Exadata Cloud@Customer

Предотвращение, обнаружение и реагирование на несанкционированные действия для соблюдения требований политики ИТ-безопасности.

14 мая, 2021 г. | Версия 2.03

ЗАЯВЛЕНИЕ О ЦЕЛИ

Данный документ содержит обзор функций и усовершенствований, внесенных в релиз 19.2.13.0.0.200428. Он составлен исключительно с тем, чтобы помочь Вам оценить пользу, которую принесет Вашему бизнесу переход на 19.2.13.0.0.200428, и спланировать проекты в области ИТ.

В этом документе обобщены функции безопасности и контроля сервиса Oracle Gen 2 Exadata Cloud@Customer (ExaC@C), предоставляемого через модуль управления Oracle Cloud Infrastructure (OCI) 2-го поколения. Документ предназначен для сотрудников службы безопасности заказчиков, привлеченных к оценке внедрения ExaC@C. Для предоставления сервиса заказчик должен согласиться со следующими положениями:

- Oracle выбирает персонал, которому разрешено подключаться к инфраструктуре ExaC@C
- Oracle предоставляет идентификационные данные персоналу для доступа к инфраструктуре ExaC@C
- Персонал Oracle, имеющий право доступа к инфраструктуре ExaC@C, будет использовать предоставленное Oracle программное обеспечение и оборудование для получения доступа к инфраструктуре

Сотрудникам службы безопасности, уполномоченным оценивать ExaC@C, следует также ознакомиться со следующей документацией, в которой описаны дополнительные средства управления, доступные с помощью Oracle Operator Access Control (OpCtl) и модуля управления Oracle Cloud Infrastructure:

- Руководство по обеспечению безопасности Exadata Cloud@Customer
- Документация по продуктам Oracle для контроля доступа операторов
- Архитектура безопасности Oracle Cloud Infrastructure

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.

Вследствие особенностей архитектуры продукта может оказаться невозможным безопасное включение всех компонентов, описанных в этом документе, без риска существенной дестабилизации программного кода.

СОДЕРЖАНИЕ

СПИСОК ИЗОБРАЖЕНИЙ

СПИСОК ТАБЛИЦ

ВВЕДЕНИЕ

Exadata Cloud@Customer (ExaC@C) предоставляет общедоступный облачный сервис Exadata Cloud в центре обработки данных заказчика с использованием принадлежащей и управляемой Oracle инфраструктуры, расположенной в центре обработки данных заказчика. Преимущество ExaC@C заключается в том, что заказчик сохраняет физический контроль над оборудованием ExaC@C, размещая его в любом центре обработки данных по своему выбору и получая при этом возможности автоматизации и эффективной работы модуля управления Oracle Cloud Infrastructure (OCI) и поддержки персонала OCI Cloud Ops для обслуживания инфраструктуры.

ExaC@C — это идеальный выбор для использования в случае, когда заказчики стремятся получить операционные и финансовые преимущества облачного решения, соблюдая политики, юридические и нормативные требования, предъявляемые к критически важным приложениям и отраслям с жестким регулированием. Например, ExaC@C отлично подходит для применения в сфере банковских и финансовых услуг, энергетики и обороны, а также в любых других сферах, где управление рисками является ключевым элементом успеха. Заказчики, работающие в этих отраслях и заинтересованные в реализации облачной стратегии, должны убедиться, что выбранный ими поставщик облачных услуг предоставляет всестороннюю поддержку этих возможностей в рамках своего стандартного предложения услуг.

Модель предоставления сервиса ExaC@C — это стандартизированное предложение, основанное на лучших отраслевых практиках защиты данных заказчиков и критически важных нагрузок. Чтобы заказчику было легче адаптироваться к модели предоставления сервисов ExaC@C, ExaC@C включает средства управления безопасностью, описанные в этом документе, в качестве компенсационных мер в крайних случаях, когда стандарты безопасности, утвержденные заказчиком, могут отличаться от модели ExaC@C. Цель этого документа — описать средства управления, чтобы они могли использоваться группами безопасности заказчика для предоставления исключений для прошлых стандартов и для создания будущих стандартов на основе этих средств управления.

СООТВЕТСТВИЕ НОРМАТИВНЫМ ТРЕБОВАНИЯМ

Стандарты соответствия операций ExaC@C нормативным требованиям и модулем управления OCI регулируются процессами и процедурами внутренней поддержки Oracle. ExaC@C имеет сертификаты соответствия (AoC) по следующим стандартам:

- ISO 27001
- Средства управления системами и организациями 1 (SOC 1)
- Средства управления системами и организациями 2 (SOC 2)
- Средства управления системами и организациями 3 (SOC 3)
- Закон об ответственности и переносе данных о страховании здоровья граждан (HIPAA)
- PCI DSS

Oracle может предоставить заказчикам определенные документы AoC по запросу заказчика. Заказчики могут запросить документы AoC у торгового представителя Oracle.

ГЛОБАЛЬНАЯ ПОЛИТИКА БЕЗОПАСНОСТИ ORACLE

Политики безопасности Oracle охватывают управление безопасностью как внутренних операций Oracle, так и сервисов, включая сервис ExaC@C, который Oracle предоставляет своим заказчикам, и действуют для всего персонала Oracle, например, сотрудников и подрядчиков. Эти политики соответствуют стандартам ISO/IEC 27002: 2013 (в прошлом ISO/IEC 17799: 2005) и ISO/IEC 27001: 2013 и определяют все области безопасности в Oracle. Oracle выполняет процедуры безопасности, опубликованные по адресу https://www.oracle.com/corporate/security-practices/corporate/. В опубликованной информации в том числе отражены следующие моменты:

- Цель — защитить конфиденциальность, целостность и доступность как данных Oracle, так и данных заказчиков
- Безопасность человеческих ресурсов
- Контроль доступа
- Безопасность сетевых коммуникаций
- Безопасность данных
- Безопасность ноутбуков и мобильных устройств
- Физическая безопасность и безопасность окружающей среды

Если Oracle работает на объекте заказчика или в его системах по его указанию, консультанты и персонал службы поддержки Oracle будут соблюдать процедуры заказчика в соответствии с соглашением между Oracle и заказчиком.

РАЗДЕЛЕНИЕ ОТВЕТСТВЕННОСТИ

Управление ExaC@C осуществляется совместно заказчиком и Oracle. Развертывание ExaC@C разделено на 2 зоны ответственности:

- Сервисы, управляемые заказчиком: компоненты, к которым заказчик имеет доступ в рамках своей подписки на ExaC@C
  - Виртуальные машины (ВМ), доступные заказчику
  - Сервисы баз данных, доступные заказчику
- Инфраструктура, управляемая Oracle: оборудование, принадлежащее и управляемое Oracle, на котором выполняются сервисы, к которым есть доступ у заказчика
  - Блоки распределения питания (PDU)
  - Коммутаторы внешнего управления (OOB)
  - Коммутаторы сетей хранения
  - Серверы Exadata Storage
  - Физические серверы Exadata Database

Заказчики контролируют и отслеживают доступ к своим сервисам, включая сетевой доступ к своим виртуальным машинам (через виртуальные сети уровня 2 и брандмауэры, реализованные в виртуальной машине заказчика), аутентификацию для доступа к виртуальной машине и аутентификацию для доступа к базам данных, запущенным на виртуальных машинах. Oracle контролирует и отслеживает доступ к компонентам управляемой инфраструктуры Oracle. Персонал Oracle не имеет доступа к сервисам заказчика, в том числе к виртуальным машинам и базам данным. В таблице 1 представлено описание разделение ответственности Oracle и заказчика.

Таблица 1. Разделение ответственности

РАБОЧАЯ ФУНКЦИЯ	ИНФРАСТРУКТУРА, УПРАВЛЯЕМАЯ ORACLE		СЕРВИСЫ, УПРАВЛЯЕМЫЕ ЗАКАЗЧИКОМ	
	Oracle Cloud Ops	Заказчик	Oracle Cloud Ops	Заказчик
Мониторинг	Инфраструктура, модуль управления, сбои оборудования, доступность, емкость	Обеспечение доступа к сети для поддержки мониторинга и сбора журналов инфраструктуры Oracle	Доступность инфраструктуры для поддержки мониторинга сервисов заказчика	Мониторинг ОС, баз данных, приложений заказчика
Управление инцидентами и их устранение	Управление инцидентами и их устранение Запасные части и отправка на места	Помощь в диагностике на месте (например, устранение неполадок в сети)	Поддержка в устранении любых инцидентов, связанных с базовой платформой	Управление инцидентами и их устранение для приложений заказчика
Управление обновлениями	Проактивная установка обновлений в оборудование и средства управления IaaS/PaaS	Обеспечение доступа к сети для поддержки обновлений	Установка доступных обновлений (например, набор обновлений Oracle DB)	Обновление экземпляров пользователей Тестирование
Резервное копирование и восстановление	Резервное копирование и восстановление инфраструктуры и модуля управления, воссоздание ВМ заказчика	Обеспечение доступа к сети для поддержки облачной автоматизации	Обеспечение работающих и доступных заказчику ВМ	Моментальные снимки / резервное копирование и восстановление данных заказчика IaaS и PaaS с использованием собственных возможностей Oracle или сторонних производителей
Поддержка облачных сервисов	Реагирование на запросы на обслуживание и решение вопросов, связанных с инфраструктурой и подпиской	Отправка запросов на обслуживание через MOS	Реагирование на запросы и устранение проблем	Отправка запросов через портал поддержки

АРХИТЕКТУРА СЕРВИСА EXAC@C

На рис. 1 представлена блок-схема архитектуры сервиса Gen 2 ExaC@C.

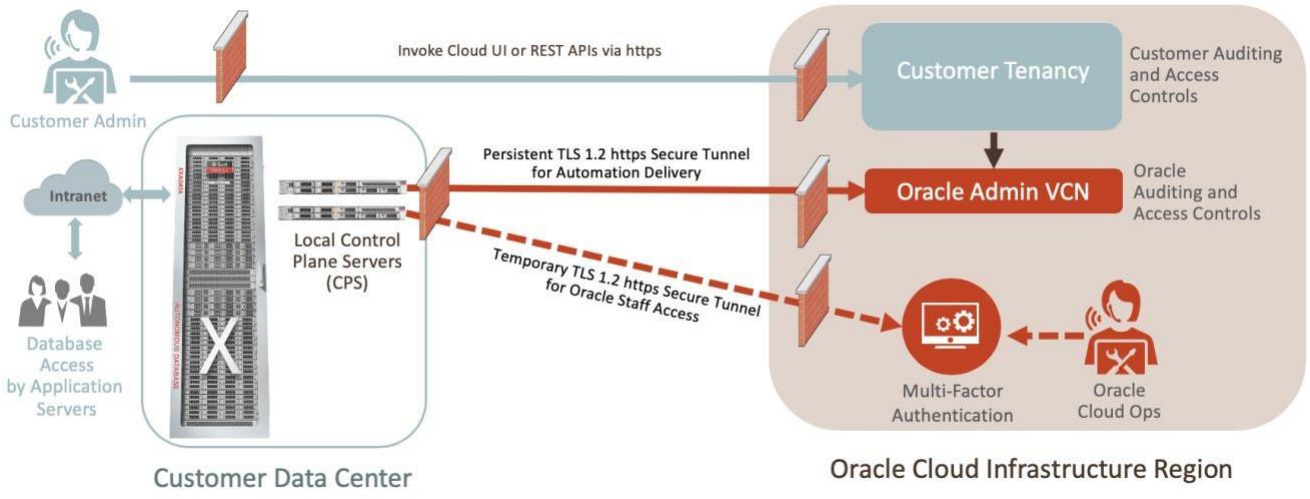

Рис. 1. Блок-схема архитектуры Oracle ExaC@C

Сервис ExaC@C развертывается в стойке ExaC@C в центре обработки данных, выбранном заказчиком. В стойке ExaC@C размещаются все компоненты стандартной машины Exadata Database Machine, а также 2 сервера модуля управления (CPS) в конфигурации высокой доступности (HA), подключенные к региону OCI.

Данные базы данных заказчика надежно защищены в локальной стойке ExaC@C, и весь доступ к базам данных заказчика осуществляется через сетевые соединения (интранет), когда заказчик дает разрешение на доступ к конкретным виртуальным машинам и базам данных в стойке ExaC@C. Учетные данные для доступа к виртуальным машинам и базам данных заказчика сохраняются и контролируются заказчиком. У заказчика есть привилегированный доступ (например, root, SYS) к своим виртуальным машинам и базам данных; он может работать с этими учетными данными, чтобы защитить виртуальную машину и базу данных и обеспечить соответствие локальным политикам и нормативным требованиям. Это включает в себя, помимо прочего, установку агентов, пересылку журналов аудита операционной системы и базы данных в систему управления информационными событиями безопасности заказчиков (SIEM), а также контроль доступа и управление идентификацией для виртуальных машин и баз данных с помощью инструментов, совместимых с операционной системой виртуальной машины ExaC@C и базой данных Oracle.

Удаленное предоставление сервиса ExaC@C, включая управляемую заказчиком облачную автоматизацию для управления базами данных и систем, а также обслуживание и поддержку инфраструктуры, выполняется в регионе OCI. Заказчик контролирует доступ к функциям управления облачной автоматизацией через сервис OCI Identity and Access Management (IAM), а сервис аудита OCI предоставляет заказчику запись всех инициированных им действий управления, запущенных через консоль OCI или конечные точки OCI REST, например, создание или удаление баз данных. Oracle контролирует сетевой доступ из региона OCI к серверу модуля управления, а также доступ оператора для выполнения обслуживания и поддержки инфраструктуры.

Сетевые подключения сервера модуля управления

Сервису ExaC@C не требуется входящее TCP-подключение для предоставления услуг, поддержки или управления. Сервису ExaC@C требуются исходящие TCP-подключения через порт 443 к конечным точкам Oracle для удаленной доставки и управления следующими сервисами Oracle:

- Сервис OCI Persistent Secure Tunnel для инфраструктуры ExaC@C
  - Обеспечение облачной автоматизации посредством вызовов REST API для автоматизации инфраструктуры ExaC@C
- Сервис OCI Persistent Secure Tunnel для выделенной автономной базы данных (ADB-D)
  - Обеспечение автоматизации облачных сервисов посредством вызовов REST API для оверлея ADB-D на инфраструктуре ExaC@C
- Сервис OCI Temporary Secure Tunnel для доступа оператора к инфраструктуре ExaC@C
  - Доступ оператора Oracle к компонентам управляемой Oracle инфраструктуры ExaC@C
- Сервис OCI Temporary Secure Tunnel для оверлея ADB-D на инфраструктуре ExaC@C
  - Доступ оператора Oracle к управляемому Oracle оверлею ADB-D на инфраструктуре ExaC@C

- Сервис OCI Monitoring
  - Метрики мониторинга инфраструктуры (например, работоспособность компонентов оборудования, обнаружение вторжений и т. д.)
- Сервис OCI Object Storage
  - Доставка обновлений ПО
- Сервис OCI Identity
  - Аутентификация и авторизация для доступа к компонентам инфраструктуры

ExaC@C поддерживает фильтрацию IP-адресов. Конкретные сервисы Oracle в определенном регионе OCI должны быть внесены в белый список, как указано в OSN CIDR для общедоступных IP-адресов, приведенных на странице https://docs.cloud.oracle.com/iaas/tools/public_ip_ranges.json. Для будущих функций ExaC@C может потребоваться доступ CPS к другим конечным точкам сервиса OCI, а IP-адреса сервисов OCI могут изменяться в диапазоне IP-адресов, перечисленных в вышеупомянутом документе. Для согласования с будущими версиями сервисов и сервисного обслуживания заказчики должны разрешить исходящий доступ CPS ко всем IP-адресам OCI, перечисленным в OSN CIDR для их региона.

ExaC@C поддерживает прокси-сервер http (например, корпоративный прокси-сервер, пассивный прокси-сервер) для управления подключениями CPS к конечным точкам OCI. Прокси-сервер http усложняет развертывание и обслуживание, чтобы обеспечить поддержку будущих версий ExaC@C, которым может потребоваться доступ к дополнительным конечным точкам OCI. Если заказчики захотят разрешить выборочный доступ к URL-адресам определенных сервисов OCI, то если Oracle добавит новые функции и услуги в ExaC@C, заказчикам может потребоваться обновить разрешенные URL-адреса.

Чтобы задать самые серьезные ограничения для сервера модуля управления ExaC@C для доступа к OCI, нужно разрешить доступ только к определенным конечным точкам в определенной области с целью предоставления сервиса ExaC@C. Для поддержки ExaC@C используются следующие URL-адреса для конечных точек Oracle:

- Сервис OCI Identity
  - https://identity.<region>.oraclecloud.com
  - см. https://docs.cloud.oracle.com/en-us/iaas/api/#/en/identity/20160918/
- Сервис OCI Object Storage
  - https://objectstorage.<region>.oraclecloud.com
  - https://swiftobjectstorage.<region>.oraclecloud.com
  - см. https://docs.cloud.oracle.com/en-us/iaas/api/#/en/objectstorage/20160918/
- Сервис OCI Monitoring
  - https://telemetry-ingestion.<region>.oraclecloud.com
  - см. https://docs.cloud.oracle.com/en-us/iaas/api/#/en/monitoring/20180401/
- Сервис ExaC@C Persistent Secure Tunnel для автоматизации доставки
  - https://wss.exacc.<region>.oci.oraclecloud.com
  - https://wsshe.adbd-exacc.<region>.oci.oraclecloud.com
- Сервисы ExaC@C Temporary Secure Tunnel для доступа оператора:
  - https://mgmthe1.exacc.<oci_region>.oci.oraclecloud.com
  - https://mgmthe2.exacc.<oci_region>.oci.oraclecloud.com
  - https://wsshe.adbd-exacc.<region>.oci.oraclecloud.com

Сервис OCI Identity, сервис Object Storage и сервис Monitoring — это общедоступные интерфейсы OCI, защищенные сертификатами с подписью CA. Сервисы ExaC@C Persistent Secure Tunnel и Temporary Secure Tunnel — это конечные точки с общедоступными IP-адресами для защищенного взаимодействия между сервером модуля управления и OCI, и эти интерфейсы защищены самозаверяющими сертификатами Oracle.

Сервис ExaC@C Persistent Secure Tunnel для автоматизации доставки используется для удаленной доставки команд облачной автоматизации (исключительно для вызовов REST API). Этот сервис предоставляется только в рамках ExaC@C и не входит в общедоступные сервисы OCI. URL-адреса для этого сервиса относятся к региону OCI, настроенного для управления инфраструктурой ExaC@C. Эти URL-адреса защищены самозаверяющими сертификатами.

Сервис ExaC@C Temporary Secure Tunnel для доступа оператора используется исключительно для доступа оператора Oracle (по протоколу ssh) к управляемой Oracle инфраструктуре ExaC@C и ресурсам ADB-D (если применимо). Этот сервис предоставляется только в рамках ExaC@C и не входит в общедоступные сервисы OCI. URL-адреса для этого сервиса относятся к региону OCI с настройками, разрешающими доступ оператора к инфраструктуре ExaC@C. Сервис OCI Temporary Secure Tunnel — это единственный способ, с помощью которого оператор Oracle может воспользоваться ssh-подключением для доступа к инфраструктуре ExaC@C и сервисам ADB-D (если применимо). Эти URL-адреса защищены самозаверяющими сертификатами.

Сертификаты для TLS-подключения управляются эксклюзивно Oracle и меняются каждые 90 дней. Заказчикам не разрешается управлять сертификатами или проверять трафик, проходящий по защищенным подключениям.

CPS требует предоставляемый заказчиком DNS для разрешения IP-адресов, сервер NTP для синхронизации часов и маршрутизацию на URL-адреса сервиса OCI.

Доступ заказчика к сервисам ExaC@C

Заказчики получают доступ к базам данных (БД) Oracle, работающим на ExaC@C, через подключение уровня 2 (теггированная сеть VLAN) с оборудования заказчика к базам данных, работающим на виртуальной машине заказчика, с использованием стандартных методов подключения к базе данных Oracle, таких как Oracle Net через порт 1521. Заказчик получает доступ к виртуальной машине, на которой запущены базы данных Oracle, с помощью стандартных методов Oracle Linux, таких как ssh на основе токена через порт 22.

Действия по управлению компонентами инфраструктуры, такие как масштабирование OCPU и создание кластера виртуальных машин (ВМ), выполняются заказчиком с использованием программного обеспечения облачной автоматизации в арендуемой среде, разработанной с учетом требований безопасности и размещенной в Oracle Cloud Infrastructure. Заказчикам не нужно управлять инфраструктурным уровнем, поскольку Oracle в соответствии со SLO обеспечивает показатель безотказной работы 99,95 %. Заказчики не могут напрямую обращаться к инфраструктуре ExaC@C, агентам мониторинга нагрузки, а также непосредственно извлекать или отправлять файлы в управляемую инфраструктуру Oracle в сервисе ExaC@C.

Реализация физической сети

На рис. 2 представлена реализация физической сети для ExaC@C. Компоненты, доступные заказчику и контролируемые им, показаны синим, в компоненты, управляемые Oracle, — красным. Компоненты инфраструктуры ExaC@C, показанные красным, соединены между собой через изолированную сеть управления уровня 2, также показанную красным. Прямого сетевого доступа из сети управления к сетям клиентов и резервного копирования нет.

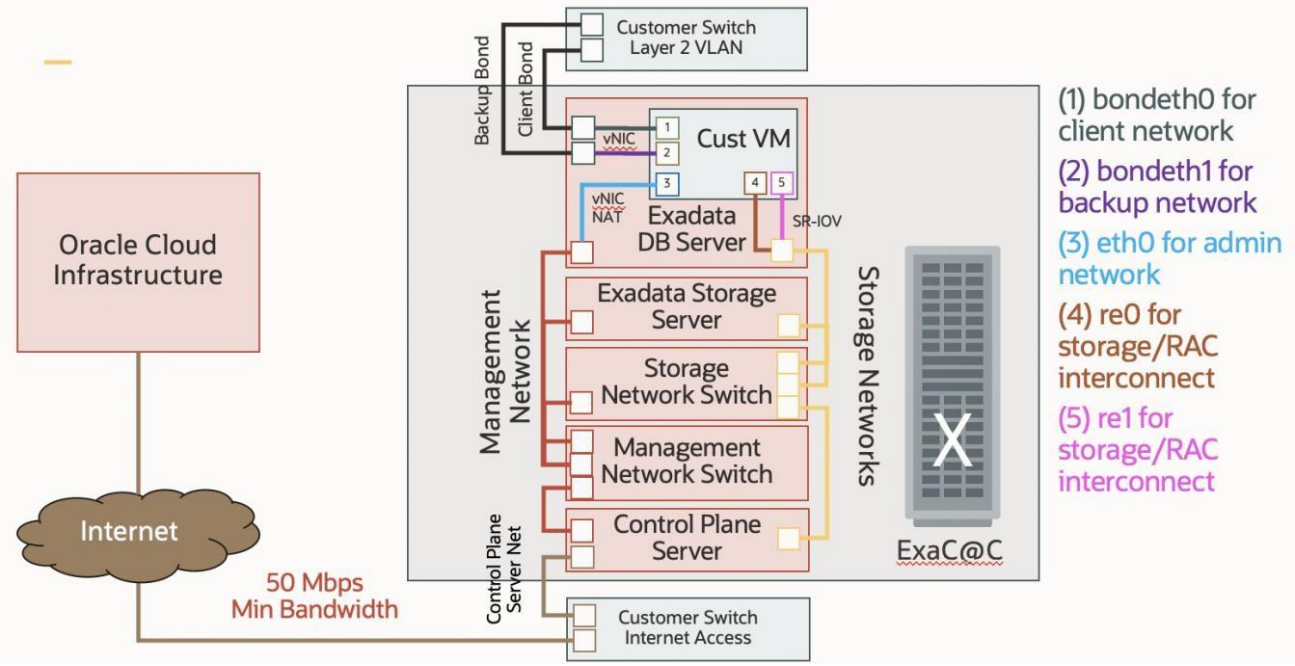

Рис. 2. Реализация физической сети ExaC@C

На рис. 3 подробно представлено, как изолирована сеть между разными кластерами виртуальных машин (кластеры ВМ), развернутыми на одном сервере базы данных ExaC@C Exadata Database (сервер DB). Когда настроено несколько кластеров виртуальных машин, заказчик контролирует теги VLAN и конфигурацию IP-сети для каждого кластера виртуальных машин, а одни и те же физические каналы используются совместно для сетей клиента (обозначается как сеть 1) и сетей резервного копирования (обозначается как сеть 1) для каждой виртуальной машины на одном и том же сервере Exadata DB. Заказчики могут указать разные теги VLAN для разных сетей в разных кластерах виртуальных машин, чтобы изолировать сетевой доступ к кластеру виртуальных машин. Внутренние сети хранения каждого кластера виртуальных машин (сети 4 и 5) изолированы с помощью средств управления уровня 2 в реализации конвергентной сети Ethernet, которая поддерживает внутреннюю сеть хранения данных, поэтому разные виртуальные машины на одном сервере базы данных Exadata никоим образом не смогут получать доступ друг к другу через внутреннюю сеть хранения. Сетевой доступ администратора vNIC / NAT (сеть 3) реализован в виде

изолированной сети /30, поэтому разные виртуальные машины на одном сервере Exadata DB никоим образом не могут получить доступ друг к другу в сети администратора.

Помимо изоляции сети, процессорные ресурсы, в качестве превентивной меры для предотвращения доступа к кэшированным данным BM с других виртуальных машин, закреплены за конкретными виртуальными машинами на данном сервере базы данных Exadata Database.

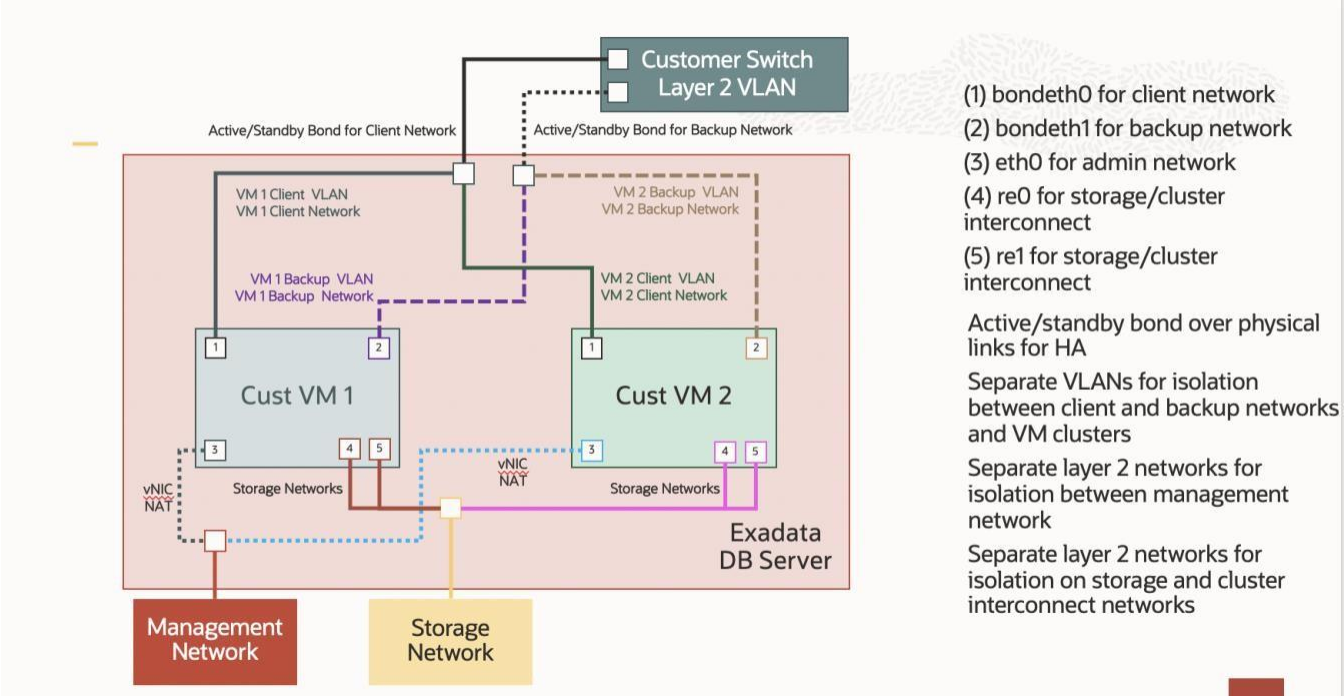

Рис. 3. Изоляция сети кластеров BM

Сервер модуля управления получает доступ к модулю управления Oracle Cloud Infrastructure (OCI) из общедоступного Интернета. Сервер модуля управления выходит в Интернет через Ethernet-подключение уровня 2 с коммутатором, управляемым заказчиком. Заказчик предоставляет службы времени (NTP), разрешение имен (DNS) для имен хостов в Интернете (например, oracle.com) и маршрутизацию (шлюз по умолчанию) для подключения сервера модуля управления к модулю управления OCI. Для сервера модуля управления не требуется входящих TCP-подключений, а требуются только исходящие подключения к IP-адресам Oracle на TCP-порту 443, описанные в разделе «Сетевые подключения сервера модуля управления» этого документа. Заказчики могут и должны устанавливать правила доступа к сети, чтобы запретить входящий доступ к серверу модуля управления и разрешить исходящий доступ только к требуемым конечным точкам Oracle. Минимально необходимая полоса пропускания для подключения с CPS к модулю управления OCI составляет 50 Мбит/с для скачивания и 10 Мбит/с для загрузки.

Сервер базы данных Exadata Database (DB) подключен к управляемому заказчиком коммутатору через Ethernet 10 Гбит/с или 25 Гбит/с, выделенному синим. Заказчик имеет доступ к своим виртуальным машинам (виртуальной машине заказчика) через пару (клиентское и резервное) сетевых подключений уровня 2 (тегированная сесть VLAN) к виртуальной машине заказчика, которые реализованы в виде виртуальных сетевых интерфейсных карт (vNIC). Физические сетевые подключения реализованы для обеспечения высокой доступности в конфигурации активный / резервный.

Виртуальная машина заказчика получает доступ к хранилищу Exadata через частную немаршрутизируемую взаимозависимую сеть через сопоставленные интерфейсы SR-IOV, показанную желтым. У каждого физического сервера базы данных Exadata Database и сервера хранения Exadata Storage есть подключение высокой доступности (активное/резервное) к паре резервных сетевых коммутаторов сети хранения. Следующий CIDR описывает стандартную IP-адресацию для конфигурации сети хранения: 100.107.0.0/24. Если эти IP-адреса конфликтуют с существующими IP-адресами, заказчики могут заменить этот блок CIDR произвольным диапазоном IP-адресов, предоставленным заказчиком.

Oracle Cloud Automation получает доступ к виртуальной машине заказчика через NAT-адрес в сети управления, реализованной на vNIC на сервере базы данных Exadata Database, показанном красным. Доступ Oracle Cloud Automation к BM заказчика контролируется по протоколу ssh на основе токена.
Oracle Cloud Automation генерирует временные уникальные пары ключей ssh для доступа к виртуальной машине заказчика для каждого действия управления, инициированного заказчиком. Открытый ключ вводится сервисом облачной автоматизации через агента DBCS в файлы `~/.ssh/authorized_keys` необходимой учетной записи сервиса в BM заказчика, например `oracle`, `opc` или

`root`. Временные закрытые ключи, используемые для автоматизации, хранятся в памяти программного обеспечения Oracle Cloud Automation, работающего на оборудовании ExaC@C в центре обработки данных заказчика, и удаляются после завершения действия. Аналогичным образом программное обеспечение облачной автоматизации удаляет временный открытый ключ из учетной записи сервиса после завершения действия.
Средства OCI Identity and Access Management (IAM) заказчика определяют, может ли и каким образом может заказчик использовать функциональные возможности Oracle Cloud Automation в отношении виртуальной машины и баз данных заказчика. На виртуальной машине заказчика есть средства обнаружения доступа, реализованные через систему аудита Oracle Linux, включая обнаружение доступа ssh с помощью облачной автоматизации. Заказчики могут блокировать доступ по протоколу ssh для облачной автоматизации на уровнях 3 и 4 через конфигурацию брандмауэра в виртуальной машине заказчика; однако это нарушит функциональность облачной автоматизации, которая должна получать доступ к виртуальной машине заказчика через ssh. Эта функциональность включает следующие возможности.

- Изменение размера группы дисков ASM
- Изменение размера локального хранилища
- Изменение размера памяти BM заказчика
- Обновление базы данных
- Обновление инфраструктуры Grid
- Обновление ОС BM

Заказчик может временно восстановить доступ к Oracle Cloud Automation, чтобы разрешить некоторые функции, необходимые для доступа к своей виртуальной машине и базам данных. Oracle Cloud Automation не требует сетевого доступа к виртуальной машине заказчика для выполнения масштабирования OCPU, а функция масштабирования OCPU будет работать нормально, когда заказчики блокируют сетевой доступ Oracle Cloud Automation к виртуальной машине заказчика.

Предоставление сервиса ExaC@C

На рис. 4 представлены порты и протоколы TCP, используемые для предоставления сервиса ExaC@C. Важные компоненты удаленного предоставления сервиса включают:

- Доступ заказчика в арендуемую область Oracle Cloud Infrastructure (OCI)
- Контроль доступа заказчика к интерфейсам пользователя и API-интерфейсам инфраструктуры OCI
- Доступ модуля управления базой данных OCI к ExaC@C для удаленной автоматизации доставки
- Сервис Secure Outgoing Tunnel для подключения ExaC@C к области OCI
- Сервис OCI Object Storage для доставки обновлений ПО компонентам ExaC@C
- Мониторинг инфраструктуры
- Управление идентификацией персонала Oracle Cloud Ops
- Временный (эфемерный) сервис защиты туннеля для доступа оператора Oracle (обратный туннель ssh)

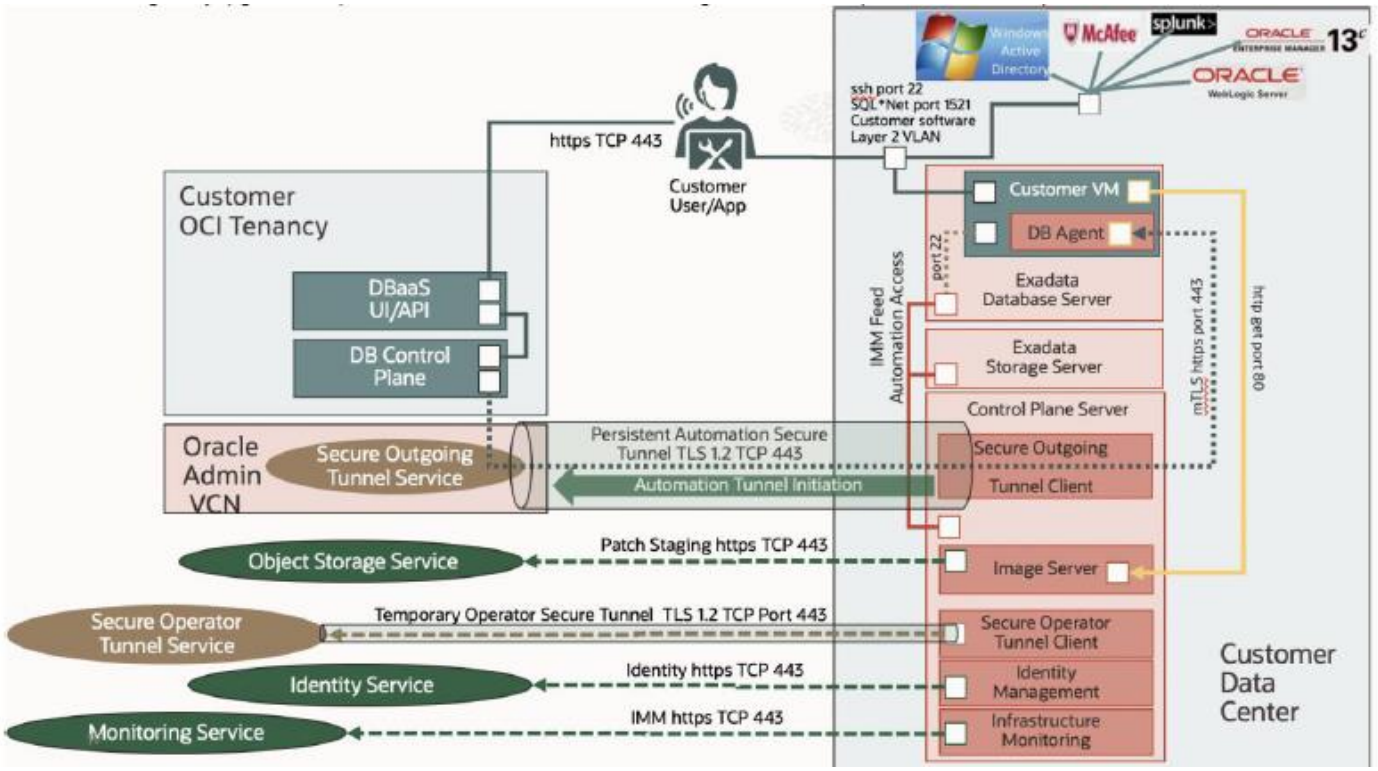

Рис. 4. Порты и протоколы сервиса ExaC@C

Сервисы ADB-D могут выполняться на сервисе ExaC@C. При развертывании сервисов ADB-D к сервису ExaC@C применяются следующие обновления.

- ВМ заказчика становится ВМ ADB-D, а у Oracle остается право войти в ВМ ADB-D (ssh на основе токена для именованного пользователя) для поддержки сервиса ADB-D; заказчики могут не иметь доступа к ВМ ADB-D согласно определению сервиса ADB-D
- Второй сервис Secure Outgoing Tunnel Service устанавливается на специфичную для ADB-D конечную точку в целях предоставления функциональных возможностей сервиса ADB-D

Второй сервис Secure Outgoing Tunnel Service устанавливается на специфичную для ADB-D конечную точку, чтобы разрешить Oracle ADB-D поддерживать доступ операторов по протоколу ssh к ВМ ADB-D

Доступ заказчика к интерфейсам OCI

Заказчик получает доступ к сервисам облачной автоматизации в своей арендуемой области OCI через https-подключение на порту 443 к модулю управления OCI. Модуль управления OCI Control Plane предоставляет следующие интерфейсы управления:

- Веб-интерфейс пользователя (веб-интерфейс) — обычно для быстрых действий
- Oracle Cloud Shell — оболочка Linux непосредственно в консоли Oracle Cloud Infrastructure.
- Интерфейс командной строки OCI (OCI CLI) — обычно для программных действий из оболочки операционной системы
- REST API (комплект разработки программного обеспечения OCI, OCI SDK) — обычно для интеграции приложений
- Terraform – для «инфраструктуры как код»

Доступ ко всем интерфейсам управления контролируется заказчиком посредством политик OCI Identity and Access Management (IAM). Если учетная запись, управляемая заказчиком, авторизована для выполнения запрошенного действия, то это действие доставляется соответствующим компонентам ExaC@C следующим образом:

- DBaaS UI/API отправляет запрос в модуль управления БД через https-подключение на порте 443
- Модуль управления БД отправляет запрос через REST API на сервис прокси-сервера (CPS-прокси) через Persistent Secure Tunnel Service Admin VCN
- Сервис Persistent Secure Tunnel TLS 1.2 завершает работу в OCI Admin VCN и CPS доставляет запрос REST API прокси-серверу CPS, работающему на CPS в стойке ExaC@C
- Прокси-сервер CPS отправляет команды компонентам ExaC@C
  - Действия, требующие доступа к сервисам базы данных в виртуальной машине заказчика, отправляются агенту БД, работающему на какой-то одной или на всех виртуальных машинах заказчика (например,

до 4 виртуальных машин в половине стойки) через mTLS-подключение (порт 443) между модулем управления OCI и каждым агентом БД; это mTLS-подключение реализовано через частную сеть в стойке ExaC@C
  - Действия, требующие доступа к виртуальной машине заказчика, выполняются по протоколу ssh на основе токенов по внутренней сети управления, реализованной как NAT-адрес на виртуальной машине заказчика, доступной с сервера базы данных Exadata; открытые ssh-ключи являются временными, генерируются для инициируемого заказчиком действия управления и хранятся в файлах authorized keys пользователей oracle, opc и root на виртуальной машине заказчика; закрытые ssh-ключи являются временными, для инициируемого заказчиком действия управления и хранятся в памяти программным обеспечением Oracle Cloud Automation, работающим на оборудовании Exadata, и хранятся в центре обработки данных заказчика.
  - Действия, требующие доступа к компонентам инфраструктуры, выполняются по ssh-протоколу на основе токенов по внутренней сети управления от CPS до требуемой конечной точки (например, Exadata Storage Server, Exadata Database Server).

Oracle регулирует и контролирует использование частных токенов ssh для управления инфраструктурой и компонентами виртуальных машин заказчиков. Эти токены хранятся и надежно защищаются на сервере CPS. Токены инфраструктуры уникальны, обеспечивают доступ только к компонентам инфраструктуры (например, серверам хранения Exadata Storage, физическому серверу базы данных Exadata Database, коммутатору сети хранения) и не обеспечивают доступ к виртуальным машинам или базам данных заказчиков. Токены виртуальных машин заказчика уникальны, обеспечивают доступ только к виртуальной машине заказчика и не обеспечивают доступ к компонентам инфраструктуры.

Мониторинг инфраструктуры

Компоненты инфраструктуры ExaC@C сообщают свои метрики управления инфраструктурой (IMM) серверу CPS, а CPS передает эту информацию в Oracle для обработки. IMM-подключение выполняется по протоколу https с привязкой к конечной точке региона OCI, используемого для управления сервисом ExaC@C.

Глобальная поддержка Oracle Global Support выполняет мониторинг и обслуживание ExaC@C следующим образом:

- Автоматический мониторинг компонентов инфраструктуры Oracle Cloud@Customer отправляет метрики мониторинга инфраструктуры (IMM) через утилиту мониторинга инфраструктуры, развернутую на CPS.
  - Температура внутренних механизмов, состояние диска и т. д.
  - Подробная информация обо всех данных мониторинга публикуется на Auto Service Request Qualified Engineered Systems Products по адресу https://docs.oracle.com/cd/E37710_01/doc.41/e37287/toc.htm
- Глобальная поддержка Oracle Global Support анализирует данные мониторинга, определяет, какие события требуют исправлений, создает заявки на поддержку и назначает заявки на поддержку сотрудникам службы поддержки OCI
- После назначения им заявок сотрудники службы поддержки Cloud Ops авторизуются и направляются для выполнения необходимых действий поддержки

Обновления программного обеспечения

Стандартные ежеквартальные пакетные обновления для базы данных Oracle, сетевой инфраструктуры и операционной системы виртуальных машин заказчика размещаются Oracle в CPS из объектного хранилища OCI. Ежеквартальные обновления программного обеспечения перечислены в интерфейсах облачной автоматизации пользователя, а применение этих обновлений контролируется заказчиком с помощью инструментов и политик OCI. Доступ к обновлениям для приложения осуществляется через исходящие http-подключения (порт 80) от виртуальной машины заказчика к серверу виртуальных образов, работающему на CPS.

Стандартные ежеквартальные пакеты исправлений и обновления программного обеспечения для компонентов инфраструктуры развертываются Oracle Cloud Automation и сотрудниками Oracle в соответствии с требованиями конкретных обновлений программного обеспечения. По возможности обновления устанавливаются на работающую систему, без простоев, с помощью таких инструментов, как Linux ksplice. Если для обновления требуется перезапуск компонента, Oracle выполняет перезапуск компонента постепенно, чтобы гарантировать доступность сервиса во время процесса обновления.

ПРЕВЕНТИВНЫЙ КОНТРОЛЬ (ДОСТУП К КОМПОНЕНТАМ И ДАННЫМ)

Сервис ExaC@C предназначен для изоляции и защиты сервисов и данных базы данных заказчика от несанкционированного доступа. Сервис ExaC@C разделяет обязанности между заказчиком и Oracle. Заказчик контролирует доступ к своим сервисам, базам данных и данным базы данных. Oracle контролирует доступ к компонентам управляемой Oracle инфраструктуры.

Средства управления доступом заказчика

Заказчик контролирует доступ к своим виртуальным машинам, базам данных и данным с помощью трех типов средств управления:

- Аутентификация
  - Учетные данные для доступа к сервисам OCI, базы данных, операционные системы BM и данные баз данных
- Сеть
  - Виртуальные сети VLAN уровня 2 для доступа к BM заказчика
  - Правила доступа к сети, реализованные в операционной системе виртуальной машины заказчика и базе данных Oracle
- Шифрование
  - Шифрование от приложения до базы данных[1]
  - Шифрование от базы данных к хранилищу[2]

Контроль доступа заказчика к сервисам ExaC@C

Заказчики выполняют действия по управлению с помощью автоматизации OCI, устанавливая https-подключение к модулю управления Oracle Public Cloud в выбранном заказчиком регионе OCI. Заказчик аутентифицируется с использованием своих учетных данных OCI Identity and Access Management (IAM), а его действия контролируются с помощью разрешений OCI IAM, настроенных заказчиком для определенных ресурсов. Если пользователь заказчика авторизован для выполнения запрошенного действия по управлению на целевом ресурсе, то запрошенная команда отправляется на локальные серверы модуля управления (CPS) через сервис Persistent Secure Tunnel (TLS 1.2) для доставки в соответствующие компоненты ExaC@C.

Заказчики и приложения баз данных получают доступ к базам данных, работающим на ExaC@C, через сетевое подключение уровня 2 (тегированная VLAN), размещенное на виртуальной машине заказчика. Доступ к базам данных и операционной системе осуществляется через учетные данные, управляемые заказчиком.

Средства контроля заказчика для обеспечения безопасности данных

Сервис Oracle ExaC@C разработан, чтобы помочь защитить данные для их законного использования заказчиками и помочь защитить данные от несанкционированного доступа, включая предотвращение доступа к данным заказчика со стороны сотрудников Oracle Cloud Ops. Меры безопасности, предназначенные для защиты от несанкционированного доступа к инфраструктуре ExaC@C, виртуальным машинам заказчиков и данным базы данных Oracle, включают следующее:

- Заказчик сохраняет контроль над аутентификацией именованных и привилегированных пользователей (например, `sys`, `system`) и доступом к базе данных.
- Заказчик сохраняет контроль над аутентификацией именованных и привилегированных пользователей Linux (например, `root`, `opc`, `oracle`, `grid`) и доступом к виртуальной машине
- Доступ к виртуальной машине заказчика регистрируется операционной системой виртуальной машины, эти журналы доступны заказчику, и заказчик может отправлять их в другие системы управления информационными событиями безопасности (SIEM) по своему выбору
- Заказчик может установить агенты мониторинга и средства управления безопасностью по своему выбору в операционной системе виртуальной машины, если только эти агенты не проникают в ядро Linux и не мешают работе Exadata
- Защита сетевых подключений к базе данных Oracle обеспечивается с помощью шифрования Oracle Advanced Security Network Encryption, которое автоматически настраивается облачной автоматизацией
- Данные базы данных Oracle защищаются ключами Oracle Transparent Data Encryption (TDE)
  - Автоматически настраиваются облачной автоматизацией и хранятся в защищенном паролем файле кошелька PKCS12, хранящемся на файловой системе виртуальной машины заказчика
  - Заказчик контролирует доступ к ключам шифрования TDE с помощью пароля кошелька
  - Заказчик может переместить главный ключ TDE во внешнее хранилище ключей, например Oracle Key Vault
- Database Vault может быть настроен для защиты доступа к пользовательским данным со стороны администраторов базы данных.

[1] Автоматизация ExaC@C настраивает шифрование Oracle Native Network Encryption; заказчики могут отменить эту настройку; Oracle настоятельно рекомендует заказчикам сохранять эту настройку

[2] Автоматизация ExaC@C настраивает шифрование Oracle Transparent Data Encryption (TDE); Oracle настоятельно рекомендует заказчикам сохранять эту настройку

Средства управления для защиты данных в движении, во время обработки и в местах хранения

На рис. 5 представлены компенсирующие средства управления в базе данных Oracle, которые защищают доступ к данным заказчиков от людей или программного обеспечения, которые могут получить доступ к инфраструктуре и компонентам виртуальных машин заказчика:

- Oracle Native Network Encryption
- Oracle Database Vault[3]
- Oracle Transparent Database Encryption (TDE)[4]

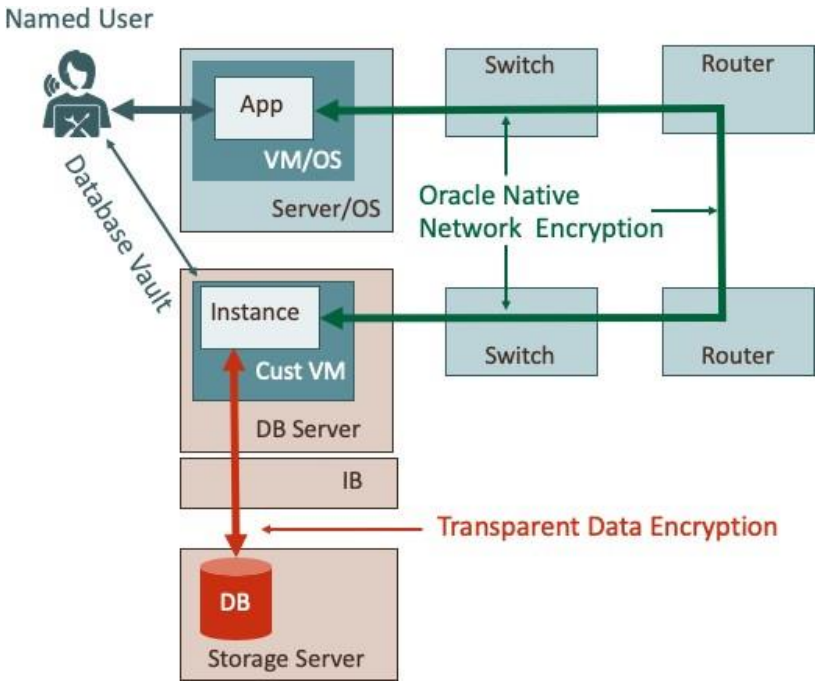

Рис. 5. Средства управления для защиты данных в движении, во время обработки и в местах хранения

Oracle Native Network Encryption

Oracle Native Network Encryption помогает защитить данные, передаваемые между приложением и экземпляром базы данных Oracle, и автоматически настраивается для баз данных, созданных с помощью автоматизации ExaC@C. Когда включено шифрование Oracle Native Network Encryption, доступ к компонентам инфраструктуры, которые могут отслеживать IP- и Ethernet-пакеты, не позволяет получить доступ к данным заказчика, поскольку эти данные зашифрованы. Документация по шифрованию Oracle Native Network Encryption публикуется в руководстве по обеспечению безопасности для каждой версии базы данных Oracle. Например, для базы данных Oracle Database 19c, см. https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-network-data-encryption-and-integrity.html

Oracle Database Vault

Средства управления безопасностью Oracle Database Vault предназначены для защиты данных приложений от доступа администратора базы данных, а также для соблюдения требований конфиденциальности и нормативных требований. Вы можете развернутьOracle Database Vault, чтобы заблокировать доступ администратора базы данных к данным приложения и управлять конфиденциальными операциями внутри базы данных, используя авторизацию доверенного пути. Oracle Database Vault помогает прозрачно защитить существующие среды баз данных без необходимости дорогостоящих и трудоемких изменений приложений. Заказчики несут ответственность за настройку и управление Oracle Database Vault с помощью программных методов Oracle Database. Документация Oracle Database Vault публикуется в руководстве администратора Oracle Database Vault, выходящем для каждой версии базы данных. Например, для базы данных Oracle Database 19c, см. https://docs.oracle.com/en/database/oracle/oracle-database/19/dvadm/introduction-to-oracle-database-vault.html .

---

[3] Включено в подписку Enterprise Edition Extreme Performance, не включено в подписку Bring Your Own License (BYOL)

[4] Включено в подписку Enterprise Edition Extreme Performance и подписку Bring Your Own License (BYOL)

Oracle Transparent Data Encryption и Oracle Key Vault

Oracle Transparent Data Encryption (TDE) шифрует данные в базе данных. Это шифрование прозрачно для авторизованных приложений и пользователей, поскольку база данных автоматически шифрует данные перед их записью в хранилище и автоматически дешифрует их при чтении из хранилища. Авторизованные приложения, которые хранят и извлекают данные из базы данных, видят только расшифрованные данные (или «открытый текст»). TDE не позволяет привилегированным пользователям операционной системы, администраторам сети и хранилища (или другим лицам, маскирующимся под них) обойти средства управления базой данных для прямого доступа к данным. Авторизованным пользователям базы данных и приложениям не нужно предоставлять ключ дешифрования при обработке зашифрованных данных. Вместо этого база данных применяет правила контроля доступа, описанные в предыдущих главах, и запрещает доступ, если пользователь не авторизован для просмотра данных.

Решение Oracle TDE разработано так, чтобы обеспечивать высокую производительность. Оно автоматически использует специальные инструкции в процессорах Intel (AES-NI) для ускорения криптографических операций. Кроме того, шифрование табличного пространства TDE без проблем работает с гибридным сжатием столбцов Exadata (EHCC) и технологией Smart Scan.

С помощью TDE конфиденциальные данные остаются зашифрованными по всей базе данных, будь то файлы хранилища табличных пространств, временные табличные пространства или undo- табличные пространства, или другие файлы, такие как redo-журналы. Кроме того, TDE может шифровать целые резервные копии базы данных и экспорт Data Pump, а Oracle Recovery Manager (RMAN) и Data Pump интегрируются с зашифрованными данными TDE.

TDE использует двухуровневую ключевую архитектуру, состоящую из ключей шифрования данных, зашифрованных с помощью главного ключа шифрования. Этот главный ключ шифрования хранится вне базы данных, по умолчанию в контейнере, совместимом с PKCS#12, который называется «кошелек», в файловой системе /u02 в операционной системе виртуальной машины заказчика, которая предоставляет общее расположение кошелька, доступное для обоих экземпляров базы данных с поддержкой RAC. Кроме того, Oracle Database 18c и более поздние версии позволяют заказчикам загружать свои собственные, сгенерированные извне ключи шифрования (Bring-Your-Own-Key, BYOK) в общий кошелек, сохраняя разделение обязанностей между администраторами баз данных и хранителями ключей. Заказчики могут выбрать миграцию своих баз данных ExaC@C в Oracle Key Vault (OKV), единственное решение управления ключами для Вашей базы данных Oracle, которое обеспечивает постоянную доступность ключей путем добавления до 16 узлов OKV в кластер управления ключами, который может охватывать географически распределенные центры обработки данных и Oracle Cloud Infrastructure (OCI). Oracle Key Vault обеспечивает непрерывное оперативное управление ключами для всех баз данных с поддержкой TDE и зашифрованных файлов изменений GoldenGate. Решение также предоставляет возможность принимать ключи, сгенерированные извне (BYOK). Подробная информация по управлению TDE публикуется в руководстве Oracle Database Advanced Security Guide для каждой версии базы данных. Например, для базы данных Oracle Database 19c, см.https://docs.oracle.com/en/database/oracle/oracle-database/19/asoag/introduction-to-transparent-data-encryption.html.

Средства управления для сетевого доступа облачной автоматизации к BM заказчика

Программное обеспечение Oracle Cloud Automation получает доступ к базам данных клиентов и виртуальным машинам клиентов с помощью двух способов

- Безопасный вход в виртуальную машину заказчика в качестве привилегированного пользователя (root, opc, oracle) по протоколу ssh на основе токенов
- Вызов REST API агента Oracle DBCS, работающего на клиентской виртуальной машине через аутентификацию mTLS на порту 443

Виртуальная машина заказчика предоставляет программное обеспечение брандмауэра Oracle Linux в качестве дополнительных компенсирующего средства для блокировки сети для виртуальной машины заказчика. Брандмауэр Oracle Linux, `iptables` или `firewalld`, блокирует доступ модуля управления на уровнях 3 (IP) и 4 (порт TCP). Заказчики могут настроить брандмауэр операционной системы для удовлетворения своих конкретных требований к безопасности.

У заказчиков нет прямого доступа к компонентам инфраструктуры для определения IP-адресов источника для конфигурации брандмауэра и для тестирования конфигурации брандмауэра виртуальной машины в целях блокировки доступа модуля управления к виртуальной машине заказчика. Заказчики должны использовать процесс подачи запросов на обслуживание Oracle (SR), чтобы запросить поддержку Cloud Ops, определить необходимые правила брандмауэра и убедиться, что конфигурация брандмауэра виртуальной машины блокирует доступ к модулю управления как необходимо

Безопасный вход Oracle Cloud Automation по протоколу ssh на основе токенов несовместим с аутентификацией Kerberos, и функциональность Oracle Cloud Automation может перестать работать, если заказчики внедряют аутентификацию Kerberos на своей виртуальной машине. Oracle не поддерживает облачную автоматизацию с Kerberos, настроенным на виртуальной машине заказчика. Дополнительные сведения см. в документе Oracle Support Document 2621025.1

(поддерживает ли виртуальная машина ExaCC аутентификацию Kerberos) по адресу: https://support.oracle.com/epmos/faces/DocContentDisplay?id=2621025.1 .

Средства управления доступом персонала заказчика к ВМ заказчика

Доступ к виртуальной машине заказчика осуществляется по протоколу ssh на основе токенов. Заказчики используют свои учетные данные и средства управления арендуемой области OCI Cloud для добавления своих специальных открытых ключей в файлы `/home/oracle/.ssh/authorized_keys` и `/home/oracle/opc/.ssh/authorized_key` пользователей `oracle` и `opc`. Персонал заказчика, имеющий доступ к закрытым ключам, ассоциированными с установленными открытыми ключами, может получить доступ к виртуальной машине заказчика по протоколу ssh на основе токенов. Oracle Cloud Automation не интегрируется с системами управления ключами заказчиков, и заказчики могут управлять ключами ssh с помощью технологии, совместимой с Oracle Linux.

Средства управления для защиты от кражи данных

Данные базы данных Oracle в базах данных Oracle ExaC@C защищаются шифрованием Oracle Transparent Data Encryption (TDE). Кража зашифрованных данных практически невозможна из-за технической сложности их дешифрования. Стандарты шифрования AES для защиты данных используются Министерством обороны США (DoD) и Агентством национальной безопасности (NSA).

Политики безопасности Oracle охватывают управление безопасностью как внутренних операций Oracle, так и сервисов, включая сервис ExaC@C, который Oracle предоставляет своим заказчикам, и действуют для всего персонала Oracle, например, сотрудников и подрядчиков. Эти политики соответствуют стандартам ISO/IEC 27002: 2013 (в прошлом ISO/IEC 17799: 2005) и ISO/IEC 27001: 2013 и определяют все области безопасности в Oracle. Oracle. Процедуры Oracle по обеспечению безопасности опубликованы по адресу https://www.oracle.com/corporate/security-practices/corporate/.

Oracle Data Safe

Oracle Data Safe — это облачный сервис безопасности, включенный в подписку Exadata Cloud at Customer. Data Safe обеспечивает:

- Доступ к конфигурации системы безопасности Вашей базы данных
- Обнаружение отклонений от конфигурации
- Выявление учетных записей с высоким риском и мониторинг их активности
- Предоставление политик аудита
- Анализ данных аудита, включая создание отчетов и предупреждений
- Обнаружение чувствительных данных, включая тип данных, их объем и местонахождение
- Маскирование чувствительных данных для непроизводственных копий баз данных, чтобы исключить риски нарушениябезопасности

Использование Data Safe не требует дополнительных затрат при условии, что число записей аудита для каждой базы данных в месяц не превысит один миллион.

Более подробную информацию о том, как Data Safe позволит улучшить безопасность среды Exadata Cloud-at-Customer, см. по адресу https://www.oracle.com/security/database-security/data-safe.

Oracle Database Security Assessment Tool (DBSAT)

Oracle Database Security Assessment Tool — это автономный инструмент командной строки, который ускоряет процесс оценки и соответствия нормативным требованиям, собирая соответствующие типы информации о конфигурации из базы данных и оценивая текущее состояние безопасности, чтобы предоставить рекомендации по снижению выявленных рисков.

DBSAT предоставляется без дополнительной оплаты и позволяет заказчикам быстро находить:

- Проблемы с конфигурацией безопасности и способы их устранения
- Пользователей и их права
- Местоположение, тип и объем чувствительных данных

DBSAT анализирует информацию о конфигурации базы данных и прослушивающем процессе (listener), чтобы определить параметры конфигурации, которые могут быть связаны с излишним риском. DBSAT выходит за рамки простой проверки конфигурации, изучая учетные записи пользователей, назначения привилегий и ролей, контроль авторизации, разделение полномочий, детальный контроль доступа, шифрование данных и управление ключами, политики аудита и разрешения файлов ОС. DBSAT применяет правила для быстрой оценки текущего состояния безопасности базы данных и получения результатов во всех перечисленных выше областях. Для каждого результата DBSAT рекомендует действия по исправлению, которые соответствуют практическим рекомендациям для снижения или компенсации риска. Применяя комплексные

измерения и компенсирующие меры, описанные в DBSAT, заказчики могут снизить риск раскрытия данных на всем предприятии.

Средства управления Oracle для доступа персонала Cloud Operations к компонентам инфраструктуры

Персонал Oracle Cloud Ops не имеет права доступа к виртуальным машинам, базам данных или данным баз данных заказчика. Персонал Oracle Cloud Operations имеет право на доступ и поддержку компонентов инфраструктуры ExaC@C, которые включают следующее оборудование:

- Блоки распределения питания (PDU)
- Коммутаторы внешнего управления (OOB)
- Коммутаторы сетей хранения
- Серверы Exadata Storage
- Физические серверы баз данных Exadata

Технические средства управления Oracle

На рис. 6 показано, как персонал Oracle Cloud Operations (Cloud Ops) получает доступ к компонентам инфраструктуры для управления ExaC@C.

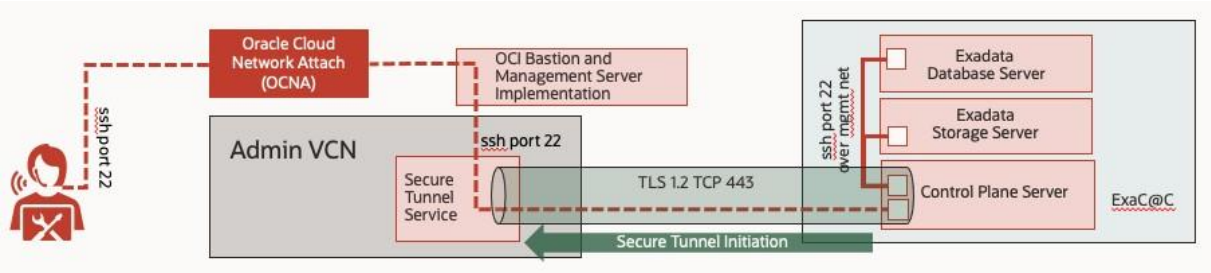

Рис. 6. Доступ персонала Cloud Operations к компонентам инфраструктуры ExaC@C

Oracle контролирует доступ персонала Oracle Cloud Ops к компонентам инфраструктуры Cloud@Customer в соответствии со следующим процессом:

- доступ к Oracle Cloud Network Attach (OCNA) с использованием FIPS 140-2 оборудования MFA (Yubikey) уровня 3 на основе правил для конкретного кода должности
- доступ к серверам Bastion и серверам управления для доступа по протоколу ssh к инфраструктуре ExaC@C
  - Доступ к серверу Bastion и проксирование через сервер Bastion доступны только в привилегированной административной инфраструктуре OCI VCN.
  - Все подключения к серверам Bastion и прокси-серверы через серверы Bastion регистрируются и отслеживаются Oracle, чтобы гарантировать выполнение авторизованных действий, недопущение неавторизованных действий и ведение исторических записей.
- Вход в инфраструктуру ExaC@C под именованным пользователем через туннель ssh с использованием MFA, реализованного с помощью аппаратного токена FIPS 140-2 уровня 3 (Yubikey)
  - Доступ к инфраструктуре ExaC@C возможен только через сервер Bastion и подсистему сервера управления
  - Личные учетные данные защищены аппаратным обеспечением Yubikey.
  - Все подключения в инфраструктуре ExaC@C контролируются Oracle, чтобы гарантировать выполнение авторизованных действий и недопущение неавторизованных действий.
- Присвоение идентификатора сервисной учетной записи или выполнение действия от имени суперпользователя (sudo), чтобы получить авторизацию сервисной учетной записи для выполнения задач управления
  - Выполнение всех команд можно отследить по конкретному именованному пользователю посредством журналирования на сервере Bastion и CPS.
  - Все подключения к компонентам инфраструктуры ExaC@C контролируются Oracle, чтобы гарантировать выполнение авторизованных действий и недопущение неавторизованных действий.

Средства управления процессами Oracle

Стандартные политики и методы обеспечения безопасности Oracle гарантируют предоставление доступа только персоналу Oracle, которому необходима эта информация и которому необходим доступ к инфраструктуре ExaC@C, и содержат следующие сведения:

- Авторизация для доступа к инфраструктуре ExaC@C возможна только для конкретного персонала службы поддержки, чьи коды должностей и записи об обучении соответствуют политикам Oracle; технические меры безопасности обеспечивают соблюдение этой политики.
- Автоматизированные процессы управления персоналом (приход/перемещение/увольнение) гарантируют, что авторизация для доступа к инфраструктуре заказчика соответствует изменениям кода должности сотрудника, записям об обучении и статусе занятости.

Средства управления и обеспечения безопасности программного обеспечения инфраструктуры Exadata

Инфраструктура ExaC@C основана на Exadata Database Machine и обеспечивает функции безопасности корпоративного класса Exadata Database Machine в локальной облачной модели. Инфраструктура ExaC@C включает следующие функции безопасности:

- Программное обеспечение, развернутое в инфраструктуре ExaC@C, ограничено минимальным набором программных компонентов, необходимых для запуска сервисов заказчика.
- Инструменты разработки и отладки для проверки данных клиентов в инфраструктуре ExaC@C не установлены.
- Несущественные инструменты и пакеты операционной системы не установлены в инфраструктуре ExaC@C
  Полную информацию о функциях безопасности Exadata Database Machine можно получить в Oracle по адресу https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/toc.htm.

ДЕТЕКТИВНЫЙ КОНТРОЛЬ (ЖУРНАЛИРОВАНИЕ И АУДИТ)

ExaC@C предоставляет комплексные средства детективного контроля (аудит и журналирование) для сервисов заказчика и управляемой инфраструктуры Oracle. Заказчик контролирует конфигурацию журналирования для сервисов заказчика, а Oracle контролирует конфигурацию журналирования инфраструктуры, управляемой Oracle. У Oracle нет разрешения на доступ к журналам аудита сервисов заказчика. Заказчик может запросить доступ к журналам аудита Oracle в соответствии с процессом Oracle подачи запроса на обслуживание (SR).

Ведение журналов аудита заказчика

ExaC@C предоставляет 3 области для аудита и журналирования действий заказчиков.

- Сервис OCI Audit: журналы аудита для действий модуля управления (например, веб-интерфейс пользователя, OCI CLI, OCI REST API), инициированных с использованием учетных данных IAM OCI заказчика
- Аудит базы данных Oracle: журналы аудита для действий базы данных, инициированных с использованием учетных данных базы данных Oracle заказчика
- Журнал аудита операционной системы виртуальной машины заказчика: журналы аудита действий, инициированных на виртуальной машине заказчика с использованием учетных данных операционной системы

Сервис Oracle Cloud Infrastructure Audit автоматически записывает вызовы на все поддерживаемые конечные точки общедоступного интерфейса программирования приложений (API) Oracle Cloud Infrastructure в виде событий журнала. В настоящее время все сервисы поддерживают журналирование с помощью Audit Logging. Журналирование событий, связанных с бакетами в сервисе объектного хранилища, поддерживается, а событий, связанных с объектами, — нет. События журналов, записываемые сервисом аудита, включают вызовы API, сделанные с консоли Oracle Cloud Infrastructure Console, из интерфейса командной строки (CLI), из набора разработчиков ПО (SDK), из Ваших собственных клиентов или других сервисов облачной инфраструктуры Oracle Cloud Infrastructure. В этих журналах содержится следующая информация:

- Время, когда произошло действие API
- Источник действия
- Цель действия
- Тип действия
- Тип ответа

Каждое событие журнала включает идентификатор заголовка, целевые ресурсы, временную отметку записанного события, параметры запроса и параметры ответа. Просматривать события, зарегистрированные сервисом аудита, можно с помощью консоли, API или SDK для Java. Данные событий можно использовать для диагностики, отслеживания потребления ресурсов, контроля соответствия нормативным требованиям и сбора событий, связанных с безопасностью. Документация о сервисе аудита OCI Audit Service опубликована по адресу https://docs.cloud.oracle.com/iaas/Content/Audit/Concepts/auditoverview.htm.

Аудит базы данных Oracle отслеживает изменения, внесенные в базу данных Oracle пользователями и не пользователями базы данных. Заказчики имеют право и обязаны настраивать журнал аудита базы данных Oracle и управлять им, в том числе отправлять журнал аудита на удаленный сервер журналов. Документация по настройке, управлению и мониторингу журналов аудита базы данных Oracle опубликована в Руководстве по безопасности базы данных Oracle для каждой версии

базы данных. Например, для базы данных Oracle Database 19c, см https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/introduction-to-auditing.html .

Журнал аудита операционной системы виртуальной машины заказчика реализован как сервис журнала аудита для операционной системы Oracle Linux (OL), работающей на виртуальной машине заказчика. Сервис журнала аудита Oracle Linux записывает действия, выполняемые с использованием учетных данных операционной системы, таких как `root`, `oracle`, `opc`, и именованных пользователей, настроенных заказчиком. Заказчики несут ответственность за настройку журнала аудита Oracle Linux в соответствии со своими стандартами, включая отправку журнала аудита Oracle Linux на удаленный сервер журналов. Документация опубликована в Руководстве по обеспечению безопасности Oracle Linux для конкретной версии операционной системы, работающей на виртуальной машине заказчика. Например, журнал аудита для дистрибутива Oracle Linux 7 опубликован по адресу https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-implement-sec.html#ol7-log-sec .

Заказчик может отслеживать доступ к сети в любой точке, которую он контролирует, включая доступ к сети между CPS и Интернетом, сетевой доступ к виртуальной машине и сетевой доступ от виртуальной машины к центру обработки данных заказчика.

Ведение журналов аудита Oracle

За ведение журналов аудита действий, предпринятых в инфраструктуре ExaC@C, принадлежащей

Oracle, отвечает Oracle. Oracle ведет следующие журналы аудита инфраструктуры для оборудования

ExaC@C X8 и более ранних версий:

- ILOM
  - `syslog`
  - Системный журнал ILOM перенаправляется в системный журнал компонента физической инфраструктуры
- Физический сервер базы данных Exadata
  - `/var/log/messages`
  - `/var/log/audit.log`
  - `/var/log/secure`
  - `/var/log/xen/xend.log`
- Сервер Exadata Storage Server
  - `/var/log/messages`
  - `/var/log/audit.log`
  - `/var/log/secure`
- Коммутатор сетей хранения
  - `/var/log/messages`
  - `/var/log/audit.log`
  - `/var/log/secure`
  - `/var/log/opensm.log`

Oracle сохраняет следующие журналы аудита инфраструктуры для оборудования ExaC@C X8M и более поздних версий оборудования:

- ILOM
  - `syslog`
  - Системный журнал ILOM перенаправляется в системный журнал компонента физической инфраструктуры
- Физический сервер базы данных Exadata
  - `/var/log/messages`
  - `/var/log/secure`
  - `/var/log/audit/audit.log`
  - `/var/log/clamav/clamav.log`
  - `/var/log/aide/aide.log`
- Сервер Exadata Storage Server
  - `/var/log/messages`
  - `/var/log/secure`
  - `/var/log/audit/audit.log`

Срок хранения журналов аудита инфраструктуры составляет 13 месяцев. Журналы аудита инфраструктуры хранятся в сервисе OCI SIEM и OCI Logging и доступны для команды Oracle DART и группы безопасности OCI. Заказчик может запросить доступ к журналам аудита инфраструктуры в соответствии с процессом Oracle подачи запроса на обслуживание (SR). Если заказчик обнаруживает подозрительную активность, нужно зарегистрировать запрос на обслуживание системы

безопасности, предоставить соответствующие журналы, что инициирует привлечение сотрудников Oracle Security Operations Center (SOC). Этот обзор выполняется независимой командой, которая вместе с заказчиком определяет «первопричину».

СРЕДСТВА УПРАВЛЕНИЯ РЕАГИРОВАНИЕМ (ПРЕРЫВАНИЕ ПОДКЛЮЧЕНИЯ)

Заказчик вместе с Oracle работают над тем, чтобы защитить и контролировать доступ к сервисам, базам данных, данным баз данных, виртуальным машинам и инфраструктуре заказчика. Если любая из сторон обнаруживает какое-либо неавторизованное действие, эта сторона может предпринять ответные действия немедленно и до уведомления другой стороны, в соответствии с политиками безопасности и в зависимости от конкретных деталей и обстоятельств неавторизованного действия. Если заказчик обнаруживает неавторизованное действие, он должен уведомить Oracle об этом действии и реакции на него в соответствии с процессом Oracle по отправке запроса на обслуживание (SR). Oracle должен уведомлять заказчика об обнаруженных неавторизованных действиях и реакции на них.

Заказчик может совершать любые ответные действия в отношении любых сервисов или оборудования, которые он контролирует. Это включает в себя прерывание сетевых подключений к виртуальной машине заказчика и прерывание сетевых подключений между ресурсами CPS и OCI. Сервисы базы данных и сами базы данных будут продолжать нормально функционировать, если заказчик прервет подключения между ресурсами CPS и OCI, а любое авторизованное действие, которое прекращается посредством такой реакции заказчика, может быть перезапущено.

Средства управления реагированием Oracle включают в себя прерывание подключений на серверах Bastion в OCI, прерывание подключений на CPS и аннулирование доступа к ресурсам ExaC@C.

РАБОЧИЕ ПРОЦЕССЫ ИСКЛЮЧЕНИЙ: ДОСТУП ORACLE К ВМ ЗАКАЗЧИКА

Сервис ExaC@C не разрешает персоналу Oracle получать доступ к виртуальной машине заказчика в нормальных рабочих условиях. Бывают исключительные случаи, когда из-за сбоя в виртуальной машине заказчика к ней требуется доступ персонала Oracle для решения проблемы. Процессы и технические средства контроля, которые определяют, как персонал Oracle может получить доступ к виртуальной машине заказчика, зависят от того, доступна ли эта виртуальная машина или нет. Процессы и технологии, применяемые в этих случаях, описаны в следующих разделах.

Сценарий 1. Заказчик может войти в свою ВМ

Если виртуальная машина заказчика доступна заказчику, то персоналу Oracle не разрешается доступ к этой виртуальной машине из компонентов инфраструктуры, управляемой Oracle. В этом случае персонал заказчика должен получить доступ к этой виртуальной машине, используя учетные данные заказчика, а затем персоналу заказчика могут предоставить совместный доступ к виртуальной машине с помощью технологии совместной работы (например, Zoom, Webex, Skype и т. д.). Такой доступ регулируется процессом отправки запроса на обслуживание следующим образом:

- Заказчик открывает запрос на обслуживание (SR) и описывает неисправность
- Заказчик или Oracle открывает сеанс общего экрана и включает информацию из этого сеанса в запрос на обслуживание
- Персонал Oracle и заказчика получает доступ к информации этого сеанса из заявки на обслуживание
- Заказчик входит в свою виртуальную машину со своими учетными данными.
- Заказчик либо вводит команды для решения проблемы в соответствии с инструкциями персонала Oracle, либо разрешает персоналу Oracle управлять вводом с клавиатуры для сеанса виртуальной машины
- Заказчик вносит в запрос на обслуживание информацию по диагностике
- Персонал Oracle вносит в запрос на обслуживание информацию по устранению проблемы

Сценарий 2. Заказчик не может войти в свою ВМ

Если заказчик не может получить доступ к своей виртуальной машине, то определенные процессы и технические средства контроля могут позволить персоналу Oracle получить доступ к виртуальной машине заказчика из инфраструктуры. Такой доступ регулируется процессом отправки запроса на обслуживание следующим образом:

- Заказчик открывает запрос на обслуживание (SR) со следующей формулировкой:
- Название запроса на обслуживание: «*Запрос на обслуживание, предоставляющий Oracle явное разрешение на доступ к DomU ExaCC с серийным номером AKXXXXXXXXX*»
- Содержание запроса на обслуживание: «*Мы открываем этот запрос на обслуживание, чтобы предоставить Oracle явное разрешение на доступ к нашему DomU для получения поддержки и решения проблемы, описанной в запросе на обслуживание # XXXXXXXX. Мы подтверждаем, что, предоставляя это разрешение, мы понимаем, что Oracle будет иметь доступ ко ВСЕМ ФАЙЛАМ в DomU, и соглашаемся с тем, что ни в одной из файловых систем DomU нет конфиденциальных файлов. Кроме того, мы также соглашаемся с тем, что служба безопасности заказчика разрешила Oracle иметь доступ к DomU заказчика для решения проблемы, описанной в вышеуказанном запросе на обслуживание».*

- Oracle или заказчик откроют общий сеанс и предоставят информацию об общем сеансе в запросе на обслуживание
- Поскольку Oracle и заказчик имеют доступ к общему сеансу, Oracle будет использовать определенные сервисные учетные записи в инфраструктуре для доступа к виртуальной машине заказчика и решения проблемы; соответствующие технические процессы будут определяться в каждом конкретном случае и в зависимости от режима сбоя, указанного в заявке на обслуживание

СРЕДСТВА УПРАВЛЕНИЯ ДОСТУПОМ ОПЕРАТОРА ORACLE

Препятствием для переноса класса приложений, поддерживающих критически важные и строго регулируемые нагрузки, на облачную платформу, является модель совместной ответственности, характерная для облачной платформы. В этой модели поставщик облачных услуг сохраняет контроль над управлением одной частью системы, например инфраструктурой (арендуемая область поставщика облачных услуг), а заказчик сохраняет контроль над другой частью системы, такой как виртуальные машины, приложения и базы данных (арендуемая область заказчика). Для критически важных и строго регулируемых нагрузок заказчик может нести ответственность за управление действиями, предпринимаемыми любым лицом при доступе к любой части системы, включая действия персонала поставщика облачных услуг в его арендуемой области. Чтобы удовлетворить эти требования, заказчики Oracle могут использовать Oracle Operator Access Control (OpCtl) с Exadata Cloud@Customer (ExaC@C) и Autonomous Database Dedicated (ADB-D) на ExaC@C.

OpCtl — это служба управления доступом между арендуемыми областями Oracle Cloud Infrastructure (OCI) для Exadata Cloud@Customer (ExaC@C). OpCtl предоставляет заказчику интерфейсы, чтобы

- Контролировать, когда и в каком объеме персонал Oracle может получать доступ к инфраструктуре ExaC@C
- Контролировать и фиксировать команды оператора Oracle и нажатие клавиш персоналом Oracle на инфраструктуре ExaC@C
- Отключать подключение оператора Oracle по усмотрению заказчика

Эти средства управления относятся к стандартным средствам сервиса ExaC@C и доступны заказчиком Oracle без дополнительной платы.

OpCtl — это подходящая функция в случаях, когда заказчикам необходимо контролировать вход персонала Oracle Cloud Ops в инфраструктуру по тем же стандартам, которые действуют для персонала заказчика, получающему доступ к управляемым системам. Например, ExaC@C отлично подходит для применения в сфере банковских и финансовых услуг, энергетики и обороны, а также в любых других сферах, где управление рисками является ключевым элементом успеха.

Функции превентивного контроля безопасности OpCtl включают:

- Доступ персонала Oracle только после авторизации заказчиком и только по конкретному рабочему запросу Oracle
- Доступ персонала Oracle ограничивается только явно одобренными компонентами, связанным с конкретным рабочим запросом
- Доступ персонала Oracle является временным и автоматически отменяется после завершения авторизованной задачи.
- Заказчик контролирует, когда персонал Oracle может получить доступ к инфраструктуре
- Программный контроль над эскалацией привилегий персонала Oracle
  Функции детективного контроля безопасности OpCtl включают:
- Уведомление заказчика, когда персоналу Oracle требуется доступ к инфраструктуре
- Журнал аудита каждой команды и нажатия клавиши, выполняемой персоналом Oracle с идентификацией конкретного сотрудника
- Мониторинг заказчиком безопасности всех команд и нажатий клавиш, производимых персоналом Oracle
- Предоставление Oracle заказчику сведений о личности сотрудника Oracle, когда это необходимо для выполнения любой команды.
- Мониторинг сотрудниками службы безопасности Oracle всех действий персонала Oracle Cloud Ops

Функции контроля безопасности реагирования OpCtl включают:

- Прекращение заказчиком доступа персонала Oracle и всех процессов, запущенных персоналом Oracle, в любое время
- Прекращение сотрудниками службы безопасности Oracle доступа персонала Oracle и всех процессов, запущенных персоналом Oracle, в любое время

Подробное описание сервиса OpCtl для инфраструктуры ExaC@C см. документацию по продукту Operator Access Control.

РЕЗЮМЕ

Функции безопасности во всей виртуальной машине и базе данных заказчика контролируются заказчиком. Функции шифрования базы данных Oracle обеспечивают шифрование данных, а заказчик сохраняет контроль над ключами шифрования. Функции безопасности базы данных Oracle управляют аутентификацией и доступом к данным в базе данных, а заказчик сохраняет контроль над этой аутентификацией и доступом. Функции аутентификации Linux управляют аутентификацией и доступом к ВМ заказчика, а заказчик сохраняет контроль над этой аутентификацией и доступом.

Функции безопасности и аудита всех управляемых Oracle компонентов сервиса ExaC@C гарантируют, что персонал Oracle Cloud Operations будет выполнять только авторизованные действия с компонентами инфраструктуры ExaC@C. Меры безопасности включают многофакторную аутентификацию именованного пользователя, надежные пароли с графиками ротации и SSH-доступ на основе токена к компонентам инфраструктуры, управляемой Oracle. Аудит и журналирование реализованы по всему стеку, а журналы аудита доступны заказчикам по запросу в соответствии с процессом Oracle по отправке заявок на обслуживание.

Благодаря сочетанию функций безопасности и аудита компонентов, управляемых заказчиком, и компонентов, управляемых Oracle, обеспечивается разделение обязанностей, а заказчик получает преимущества локального развертывания с высоким уровнем безопасности, простотой использования и экономичностью облака. Заказчики и персонал Oracle Cloud Operations вместе работают над тем, чтобы обеспечить безопасность системы и предотвратить несанкционированный доступ и кражу данных заказчиков. Персонал Oracle Cloud Operations не имеет доступа к сетям, сервисам или данным заказчиков для предоставления сервиса ExaC@C, а заказчики не имеют доступа к управляемой инфраструктуре Oracle для пользования сервисом ExaC@C. В модели развертывания ExaC@C заказчикам обеспечивается безопасность локального развертывания и преимущества экономии, гибкости и масштабируемости облачного решения.

СВЯЗАТЬСЯ С НАМИ

Позвоните по номеру +1.800.ORACLE1 или посетите сайт oracle.com.
Если вы находитесь за пределами Северной Америки, найдите местный офис на странице oracle.com/contact.

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

Средства управления безопасностью
Exadata Cloud@Customer
Май, 2021 г.
Автор: [НЕОБЯЗАТЕЛЬНО]
Соавторы: [НЕОБЯЗАТЕЛЬНО]