ORACLE IDENTITY MANAGEMENT 11*g*

ОСНОВНЫЕ ФУНКЦИИ И ПРЕИМУЩЕСТВА

ФУНКЦИИ

- **Управление учетными данными:** управление жизненным циклом учетных данных (распределение и согласование); управление операционным процессом; автоматизированное выделение учетных записей и управление паролями, выявление корпоративных ролей и управление ими.
- **Аутентификация и управление** доверительными отношениями: многофакторная, строгая аутентификация; механизм подтверждения аутентификации; единый вход; стандартизация используемых данных; конфиденциальность.
- **Контроль доступа:** авторизация с учетом оценки риска; высокоточное выделение прав, безопасность веб–служб.
- **Соответствие нормативным требованиям:** обеспечение соответствия и создание отчетности для аудита; разделение обязанностей; управление разрешением конфликтов; аттестация; аналитические функции для предотвращения мошеннических действий.
- **Удобство:** настройка на уровне отдельных служб; взаимодействие с пользователем и мониторинг окружения посредством панелей управления; автоматизация действий; управление обновлениями ПО.
- **Службы каталогов:** энергонезависимое хранение данных, виртуализация удостоверений, синхронизация; обеспечение безопасности пользователей базы данных.

ПРЕИМУЩЕСТВА

- **Завершенное решение:** полный набор лучших в своем классе средств для управления удостоверениями и контроля доступа.
- **Интеграция:** компоненты Oracle Identity Management тесно взаимодействуют друг с другом. Кроме того, компоненты программного пакета беспрепятственно интегрируются с другими приложениями Oracle (такими как Oracle PeopleSoft, Oracle E–Business Suite, Oracle Siebel) и другими компонентами Oracle Fusion Middleware (напр., Oracle WebCenter, Oracle SOA, Oracle Business Intelligence).
- **Оперативная подключаемость:** основанные на стандартах компоненты пакета Oracle Identity Management могут использоваться в разнородных окружениях, содержащих решения от разных производителей, включая операционные системы, веб–серверы, серверы приложений, серверы каталогов и системы управления базами данных.

С помощью входящего в состав Oracle Fusion Middleware 11g пакета Oracle Identity Management создается единая, интегрированная платформа безопасности, позволяющая управлять учетными данными и правами пользователей, распределять ресурсы среди пользователей, обеспечивать безопасность доступа к корпоративным ресурсам, а также контролировать результаты аудита в масштабах корпоративных приложений.

Введение

Пакет Oracle Identity Management (IM) 11*g*R1 обеспечивает защиту крупных распределенных сетей приложений, позволяя достигать нового уровня безопасности для защиты ресурсов предприятия и управления связанными процессами обеспечения безопасности. Oracle IM 11*g*R1 обладает повышенным КПД благодаря высокому уровню интеграции, консолидации и автоматизации составляющих его компонентов. Кроме того, продукт удобен в управлении и обладает повышенной эффективностью в сферах безопасности приложений, управления рисками, а также интеграции с системами управления базами данных.

Oracle IM 11*g*R1 имеет следующие преимущества по сравнению со своим предшественником (10*g*): закрепление за пакетом Oracle IM роли платформы разработки функций безопасности; улучшенная интеграция компонентов Oracle IM и других компонентов Oracle Fusion Middleware, приложений Oracle, СУБД Oracle, а также сторонних поставщиков систем безопасности; улучшенная функциональность, упрощающая развертывание в масштабах предприятия; единый для всего пакета подход к технологической инфраструктуре для критически важных функций и операций, включая установку, настройку, интерфейс пользователя, рабочий процесс и генерацию отчетов.

Компоненты Oracle Identity Management 11*g*R1

В пакет Oracle Identity Management 11*g*R1 входят следующие продукты.

Oracle Identity Manager

Oracle Identity Manager (OIM) отвечает на вопрос: "Кто получил доступ к Чему, Когда, Как, и Почему?" OIM предназначается для администрирования прав доступа в отношении всех ресурсов компании со стороны пользователей как внутренней, так и внешней сети, начиная с изначального процесса их регистрации до завершающего шага блокирования учетной записи. При использовании во внешней сети, отличная масштабируемость OIM позволяет предприятиям обеспечивать миллионам заказчиков доступ к ресурсам компании при помощи традиционных клиентов (напр. браузеров) или смартфонов.

Oracle Role Manager

Oracle Role Manager (ORM) содержит полный набор функций для управления жизненным циклом бизнес–ролей в масштабах предприятия. ORM является доверенным источником корпоративных ролей в пакете продуктов Oracle IM. Oracle Identity Manager и ORM дополняют друг друга, обеспечивая ролевой доступ при управлении правами и полонмочиями.

- Лидерство в своем классе: пакет Oracle IM характеризуется завершенностью, интегрируемостью и оперативной подключаемостью. Функциональность компонентов данного пакета делает их ведущими, лучшими в своем классе продуктами даже при обособленном использовании. Заказчики, в частности те, кто нуждается в расширенных возможностях для поддержки своей распределенной сети приложений, могут выбрать один из компонентов Oracle IM для удовлетворения своих индивидуальных потребностей, после чего интегрировать этот компонент в свой набор средств для управления удостоверениями. Или же, как вариант, они могут внедрить весь пакет Oracle IM и воспользоваться его великолепными возможностями в сфере интеграции.

Oracle Access Manager

Oracle Access Manager (OAM) предоставляет централизованные, управляемые политиками службы аутентификации, функцию единого входа (SSO), а также механизм подтверждения аутентификации. OAM интегрируется с разнообразными механизмами аутентификации, веб–серверами и серверами приложений от сторонних разработчиков, а также основанными на стандартах переносимыми решениями единого входа для обеспечения максимальной гибкости и создания интегрированного, полного решения для контроля веб–доступа. OAM дополняет собственные функции авторизации и выявления атрибутов интеграцией с Oracle Entitlements Server, позволяющей выполнять детальную авторизацию в приложениях, базах данных и веб–службах.

Oracle Web Services Manager

Oracle Web Services Manager (OWSM) для веб–служб является тем же, чем Oracle Access Manager является для веб–приложений. OWSM разработан для защиты доступа к многочисленным типам ресурсов, среди которых совместимые со стандартами веб–службы (Java EE, Microsoft .NET, PL/SQL, и т.д.); композитные приложения сервис–ориентированной архитектуры (SOA), включая процессы BPEL и процессы сервисной шины предприятия (ESB); а также удаленные портлеты Oracle WebCenter.

Oracle Identity Federation

Oracle Identity Federation (OIF) является автономным решением, позволяющим при помощи браузера выполнять кросс–доменный единый вход с использованием индустриальных стандартов (Security Assertion Markup Language – SAML, Liberty ID–FF, WS–Federation). В OIF 11*g*R1 реализована поддержка протокола Microsoft Windows CardSpace (например, провайдер удостоверений OIF может предложить пользователю выполнить вход по протоколу CardSpace, после чего вернуть подтверждение SAML, созданное на основании аутентификации и атрибутов CardSpace).

Oracle Enterprise Single Sign–On

Oracle Enterprise Single Sign–On (eSSO) – это пакет для рабочих станций Microsoft Windows. Его компоненты предоставляют функции объединенной аутентификации и единого входа для приложений "толстых" и "тонких" клиентов, не требуя модификации имеющихся приложений. Oracle eSSO позволяет корпоративным пользователям использовать единый вход для всех своих приложений, при этом пользователь может быть подключен к корпоративной сети, находиться вдали от офиса, перемещаться между компьютерами или работать на общем компьютере.

Oracle Entitlements Server

Oracle Entitlements Server (OES) является подсистемой детальной авторизации, реализующей, объединяющей и упрощающей управление сложными политиками выделения прав. OES обеспечивает безопасность доступа к ресурсам приложений и программным компонентам (таким как URL–адреса, Enterprise JavaBeans и Java Server Pages), а также к произвольным бизнес–объектам (таким как учетные записи заказчиков или информация о пациентах в базе данных). OES предоставляет централизованный пункт администрирования комплексных политик выделения прав, который может применяться в широком спектре деловых и информационно–технологических систем.

Oracle Adaptive Access Manager

Oracle Adaptive Access Manager (OAAM) защищает ресурсы, в режиме реального времени предотвращая попытки мошенничества, выполняя аутентификацию с использованием нескольких факторов, а также используя уникальный механизм усиления аутентификации. OAAM состоит из двух основных компонентов, в совокупности являющихся одним из самых мощных и гибких средств для борьбы с мошенничеством. Компонент Adaptive Strong Authenticator обеспечивает многофакторную аутентификацию и предоставляет механизмы защиты конфиденциальной информации, такой как пароли, токены, номера счетов и другие важные данные. Компонент Adaptive Risk Manager предоставляет функции анализа рисков (работающие как в режиме реального времени, так и в автономном режиме), а также позволяет выполнять операции по предотвращению мошеннических действий в критические моменты входа в систему и осуществления транзакции.

ИНТЕГРАЦИЯ КОМПОНЕНТОВ ORACLE IDENTITY MANAGEMENT

Ниже приведены примеры взаимодействия нескольких компонентов Oracle Identity Management для создания монолитного решения по обеспечению безопасности.

Интеграция Oracle Identity Manager и Oracle Role Manager

Взаимодополняемость OIM и ORM позволяет распределять и права доступа на основании ролей. Первый продукт осуществляет распределение учетных данных и управление ими, в то время как второй направлен преимущественно на управление жизненным циклом роллей.

Интеграция Oracle Access Manager и Oracle Identity Federation

Прежде всего, OAM запрашивает у пользователя идентификационные данные. После прохождения аутентификации, OAM создает cookie–файл системы единого входа (SSO) и передает проверенное удостоверение общей службе удостоверений (OIF). Служба OIF генерирует талон аутентификации (подтверждение SAML), основанный на информации, полученной от приложения OAM, после чего отправляет подтверждение SAML провайдеру услуг.

Интеграция Oracle Access Manager и Oracle Web Services Manager

Пользователь проходит аутентификацию в приложении, защищенном OAM, а приложение выполняет служебный запрос от лица пользователя. Агент OWSM–клиента перехватывает запрос и вставляет необходимую информацию системы безопасности в заголовок SOAP–сообщения (подтверждение SAML), основанную на сведениях о личности пользователя, полученных от OAM.

Интеграция Oracle Access Manager и Oracle Entitlements Manager

OAM подтверждает личность аутентифицированного пользователя и передает запрос на авторизацию приложению OES. OES извлекает информацию о доверенном объекте, запросе, сделанном в отношении ресурса, а также контексте безопасности, после чего осуществляет динамическую оценку роли. OES проверяет объект и роль на соответствие с политикой авторизации приложений, после чего выделяет узкоспециализированный доступ к ресурсам.

Интеграция Oracle Entitlements Manager и Oracle Web Services Manager

OWSM может доверить OES решение о доступе к службе путем передачи удостоверения пользователя и контекстных параметров, сообщающих OES о способе извлечения данных из самого сообщения при принятии решения о выделении прав. OES учитывает собственные политики и сведения, приведенные в сообщении, после чего возвращает OWSM ответ разрешить или отказать. OWSM может проконтролировать выполнение этого решения.

Oracle Directory Services

Oracle Internet Directory (OID) предоставляет компонентам Oracle Fusion Middleware, приложениям Oracle Fusion и внутренним корпоративным приложениям стандартизованный механизм, использующий протокол LDAP для хранения учетных данных и доступа к ним. К таким данным относятся данные идентификации пользователя (использующиеся при аутентификации), привилегии доступа (для авторизации) и сведения профиля.

Продукт Oracle Virtual Directory (OVD) разработан для осуществления агрегации и преобразования учетных данных в режиме реального времени, без копирования или синхронизации данных. OVD скрывает сложность нижестоящих инфраструктур данных, создавая основанную на LDAP и XML стандартизованную визуализацию существующих данных по корпоративным удостоверениям, при этом не перемещая данных из их исходного хранилища.

Oracle Platform Security Services

В лице продукта Oracle Platform Security Services (OPSS) корпоративные разработчики, системные интеграторы и независимые производители ПО получают основанный на стандартах, переносимый, интегрируемый каркас безопасности корпоративного уровня для приложений Java Platform, Standard Edition (Java SE) и Java Platform, Enterprise Edition (Java EE). OPSS избавляет разработчиков от задач, напрямую не связанных с разработкой приложений, предоставляя слой абстракции в виде стандартизованных API. OPSS является фундаментом безопасности для Oracle Fusion Middleware: все компоненты Oracle Fusion Middleware 11*g* и приложения Oracle Fusion используют службы OPSS.

Oracle Management Pack for Identity Management

Oracle Management Pack for Identity Management использует широкий набор возможностей Oracle Enterprise Manager для контроля монолитных окружений Oracle Access Manager, Oracle Identity Manager и Oracle Identity Federation.

Oracle Identity Management и другие технологии Oracle

Пакет Oracle Identity Management может использоваться с рядом дополняющих его технологий Oracle. В следующих разделах дается описание того, как пакет Oracle Identity Management интегрируется с технологией Oracle Information Rights Management, платформой Governance, Risk, and Compliance (GRC), а также функциями Oracle для обеспечения безопасности баз данных.

Oracle Identity Management и Oracle Information Rights Management

Технология Oracle Information Rights Management (IRM) используется для непосредственной защиты информации. Она использует "запечатывание" для уменьшения периметра контроля доступа до фактических блоков цифровой информации, таких как документы, электронные письма и веб–страницы. Oracle IRM использует следующие компоненты Oracle IM: Oracle Identity Manager для централизованного выделения прав доступа пользователям IRM; Oracle Virtual Directory для синхронизации пользователей и групп IRM из существующих на предприятии каталогов (LDAP и прочих); а также Oracle Enterprise Single Sign–On для единого входа с рабочих станций и дополнительной поддержки строгой аутентификации.

В интеграции компонентов пакета Oracle Identity Management может участвовать более двух продуктов. Например, для поддержки полнофункциональных веб–транзакций OAM может использовать узкоспециализированную авторизацию при помощи OES и одновременно с этим использовать OWSM для обеспечения безопасности запросов к внутренним и внешним веб–службам и композитным приложениям SOA.

Oracle Identity Management и Enterprise Governance

Разработанная Oracle платформа Governance, Risk и Compliance (GRC) интегрирует в себе функции бизнес–аналитики, а также функции управления процессами и автоматизированного контроля, что позволяет наладить устойчивый процесс управления рисками и соблюдения нормативного соответствия. При использовании Oracle Identity Management 11*g*R1 продукты Oracle Identity Manager, Oracle Role Manager и Oracle Access Manager встраиваются в линейку средств, используемых Oracle GRC для управления инфраструктурой. Ключевой продукт платформы Oracle GRC – Oracle Application Access Controls Governor – позволяет заказчикам управлять политиками разграничения обязанностей в рамках планирования ресурсов предприятия. Как правило, Oracle Identity Manager интегрируется с Oracle Application Access Controls Governor для утверждения в режиме реального времени политик разграничения обязанностей перед выделением ролей и ответственностей пакету Oracle E–Business.

Oracle Identity Management и Oracle Database Security

По сравнению с другими средствами управления учетными данными предложение Oracle характеризуется большей гибкостью и широтой выбора, предлагаемого заказчику. Это достигается благодаря интеграции компонента Oracle Virtual Directory (OVD) с функцией СУБД Oracle Enterprise User Security (EUS), позволяющей организациям выполнять центральное управление удостоверениями пользователей БД при помощи имеющихся корпоративных каталогов, таких как Oracle Internet Directory (OID), Microsoft Active Directory и Sun Java System Directory Server. Благодаря интеграции OVD и EUS организации могут использовать функцию виртуализации учетных данных для управления правами пользователей БД и их привилегированными ролями в рамках разнообразных хранилищ, без необходимости переноса или синхронизации данных. Кроме того, OID использует две уникальных функции безопасности баз данных: Oracle Database Vault (контролирующую разграничение обязанностей администраторов БД) и Oracle Transparent Encryption. Oracle Database Vault защищает данные удостоверений от доступа или манипуляций со стороны лиц, не имеющих доступа к протоколу OID. Функция Transparent Data Encryption выполняет шифрование данных в БД. Таким образом, даже если несанкционированный пользователь получит доступ к базе данных, он не сможет прочитать данные. Функции Oracle Database Vault и Oracle Transparent Data Encryption позволяют Oracle предлагать единственные службы каталогов, обеспечивающие полную защиту от хранилища до клиента.

Контакты

Oracle Россия
119435, г. Москва, Краснопресненская наб., 18
Москва–Сити, БЦ "Башня на набережной"
блок С
Тел.: +7 (495) 641 1400
Факс: +7 (495) 641 1414
E–mail: oracle_ru@oracle.com
Internet: www.oracle.com/ru/

191186, г. Санкт–Петербург, Невский пр., 25
Тел.: +7 (812) 363 3257
Факс: +7 (812) 363 3258

Oracle Украина
01601, г. Киев, Бизнес–центр "Парус"
ул. Мечникова, 2–а, 16 эт.
Тел.: + 380 (44) 490–90–50/51
Факс: + 380 (44) 490–90–52

Oracle Казахстан
480099, г. Алматы, микрорайон Самал–2,
Самал Тауэрс, оф. 97, блок А–2, 6–й этаж
Тел.: +7 (3272) 58 47 48/40
Факс: +7 (3272) 58 47 44

Oracle Республика Беларусь
220004, г. Минск ул. Немига, д. 40
БЦ "Немига–Сити", к. 511
Тел.: +375 172007810/11
Факс: +375 172007817

Oracle Азербайджан
AZ1065, г.Баку, ул. Джафар Джаббарли, 14,
БЦ "Каспиан Плаза III", 11 этаж