УПРАВЛЕНИЕ ПРАВАМИ ДОСТУПА К ДАННЫМ

ORACLE

ORACLE IS THE INFORMATION COMPANY

Введение

Oracle Information Rights Management (IRM) – новая технология информационной безопасности, которая контролирует использование информации и защищает её везде, где она хранится и используется. Обычные продукты по управлению информацией только управляют документами, электронными сообщениями и web-страницами, когда они хранятся в серверных репозиториях (хранилищах данных). Решение по управлению правами доступа к данным от компании Oracle использует кодирование и расширяет управление информацией за границы хранилищ для любых копий критической для организации информации, везде, где она хранится и используется – на рабочих станциях пользователей, лаптопах и мобильных переносных устройствах, в других репозиториях, внутри организации и снаружи, за пределами межсетевых экранов (вне периметра безопасности).

Oracle IRM обеспечивает безопасность самой информации, то есть напрямую защищает саму информацию, а не только хранилища, где она находится. Решение Oracle IRM, являясь одним из сервисов линейки Oracle Fusion Middleware, глубоко интегрировано в спектр решений Oracle, в частности, в Content Management, Records Management, Identity and Access Management.

Oracle Information Rights Management вводит новые элементы в жизненный цикл документооборота, такие как «запечатывание» и классификацию документов, электронной почты и web-страниц и требует установки агента на рабочие станции пользователей и на каждое устройство, на котором эта закодированная информация хранится или используется. Выгоды подхода ориентированного на защиту информации так очевидны, а изменения в привычные механизмы жизненного цикла так минимальны, что Oracle IRM повсеместно используется в организациях и государственных структурах для обеспечения безопасности наиболее конфиденциальной информации.

В данном техническом обзоре Oracle IRM детально рассматриваются вопросы о том, какие проблемы решает данное решение, как оно работает, какие ключевые моменты необходимы для успешного внедрения в крупных организациях, обсуждаются архитектуры внедрения, различные компоненты, включая средства для разработчиков.

Проблема

Основной проблемой, которую позволяет решить Oracle Information Rights Management, является возможность полного управления информацией для организаций, которые до этого могли управлять только небольшим количеством данных, хранящихся в защищённых хранилищах. Основной же объём информации оставался либо плохо управляемым, либо совсем не под контролем, так как эта информация циркулировала между серверами, рабочими станциями, лаптопами, мобильными и беспроводными устройствами, снаружи и вне межсетевых экранов.

Ограничения существующих систем безопасности

Общим методом построения систем защиты информации является опора на понятие периметра безопасности, а не на саму информацию как таковую. Документы и сообщения электронной почты до некоторой степени защищены, пока они находятся внутри контролируемых периметров, таких как файловые папки, контейнеры электронной почты, управляемые

репозитории, системы документооборота и т.д. Но когда эти документы используются на тысячах рабочих станций, лаптопах, мобильных и беспроводных устройствах внутри или вне зоны действия корпоративных межсетевых экранов, их можно легко и незаметно для администраторов открыть, скопировать, отправить... куда угодно.

Системы защиты на основе периметра безопасности занимаются информацией пока она хранится внутри периметра и передаётся. В результате такие системы имеют серьёзные ограничения:

- Традиционная безопасность прекращает своё действие на межсетевых экранах, в то время как большинству современных компаний и государственных организаций приходится отдавать свою конфиденциальную информацию наружу, делясь ею с партнёрами, клиентами, поставщиками и жителями.
- Копии одной и той же информации могут находиться внутри многих периметров с различными контролями доступа (например, прайс-лист может быть скопирован из отдела продаж в отдел маркетинга) или туда, где контроля нет совсем.
- На практике существует много различно управляемых периметров даже тогда, когда информация находится в одном месте.
- Возникают большие проблемы с попытками сделать вложенные периметры для того, чтобы делиться информацией или её разделять.

Несмотря на все инвестиции в информационную безопасность, заметным фактом является то, что, как только требуется делиться информацией, никто уже не знает, кто завтра сможет ей воспользоваться.

Ограничения на управление информацией в хранилищах

Компании инвестируют миллионы долларов в решения по управлению информацией, которые оперируют терминами безопасности, аудита, хранения документов, управления версиями и др. Эти системы управления являются преимущественно освнованными на хранилищах данных. Для того чтобы работать с этой информацией, организации хранят эти данные в управляемых репозиториях, которые могут быть базами данных (для структурированной информации), корпоративными системами управления содержимым (content management systems) или системами управления общими ресурсами (для неструктурированной информации).

Основной проблемой является то, что, когда эта контролируемая информация из хранилища используется в повседневной работе, много копий неминуемо передаются и используются вне репозитория, где уже нет возможности ими управлять. Но, кроме отсутствия безопасности и аудита вне репозитория, которое обсуждалось ранее, хорошими иллюстрациями ограниченности подхода ориентации на хранилища являются управление версиями и жизненным циклом данных:

- Управление жизненным циклом основано на политиках хранения и перемещения, например, необходимо быть уверенным, что критические для бизнеса документы сохраняются (скажем) семь лет, в течение которых их нельзя изменять, а затем они должны быть уничтожены, чтобы избежать ненужных рисков при возможных судебных расследованиях. Но, снова, при уничтожении данных в управляемых хранилищах сотни рассеянных в других местах (на других серверах и рабочих станциях) копий продолжают существовать, и их можно будет найти современными поисковыми системами.

- Системы управления содержимым предоставляют мощную поддержку управления версиями, так что пользователи легко могут получить последние версии документов. Но много пользователей всё ещё будут использовать старые версии, хранящиеся локально, вне репозитория, например, на их рабочих станциях или в почтовых ящиках. Это может привести к серьёзным ошибкам, бесполезной работе, нарушению инструкций и сбоям в текущей работе.

Фактически, решения, основанные на репозиториях, управляют только некоторой частью документов компании, тем самым, подрывая выгоды от их возможного использования. Например, приложения, в идеале приложения, работающие с информацией должны управлять всеми копиями информации, несмотря на то, где она хранится и используется.

Решение

Oracle Information Rights Management использует «запечатывание» для того, чтобы обеспечить реальный периметр управления документами электронными сообщениями и web-страницами в любом месте, где бы они не были.

Oracle называет процесс кодирования «запечатыванием», потому что он реально выполняет три функции:

- Происходит упаковывание информации слоем кодирования, так что, несмотря на то, как много копий сделано и где они хранятся, они бесполезны без соответствующих данных для раскодирования
- В кодируемый документ встраивается набор ссылок (URL links), так что каждая копия ссылается на Oracle IRM сервер, на котором информация была «запечатана»
- Используется цифровая подпись, так что любая попытка подделки документов будет определена и предотвращена

Подход, ориентированный на защиту информации

Сами права доступа на запечатанные документы хранятся отдельно от самих данных, на расположенном в сети сервере Oracle IRM, который обслуживает организация-собственник документов. Это привносит несколько революционных преимуществ, так что, где бы информация не хранилась передавалась или использовалась:

- Неавторизованные пользователи не могут получить к ней доступ (наиболее значимая выгода)
- Только авторизованные пользователи могут открывать или модифицировать документы в соответствии с их правами (например, право на распечатывание особо секретной информации)

Рисунок 1. «Запечатанная» информация остаётся управляемой в любом месте

- Вся работа с запечатанной информацией (и попытки доступа к ней) централизованно протоколируются
- Доступ к удалённо хранимой информации может быть централизованно отменён, например, если отношения с пользователем, работником по контракту, партнёром завершились (если он сделал эти копии, используя DVD, USB и др. средства)

Вероятно, наиболее уникальным свойством Oracle Information Rights Management по сравнению с другими решениями безопасности является его способность управлять информацией снаружи межсетевых экранов, даже когда информация хранится в сети других организаций или дома. Это является принципиально важным, ввиду того, что современному бизнесу необходимо вовлекать других участников, партнёров, подрядчиков, поддерживающие подразделения (например, при аутсорсинге), внешних консультантов, домашних работников и т.д.

Управление информацией вне репозитория

Решение Oracle IRM позволяет не только расширить безопасность и аудит за пределы контролируемых хранилищ данных. Оно также расширяет другие аспекты управления информацией за пределы репозитория, такие как управление жизненным циклом и версиями документов, расширяет выгоды решений по управлению документами на каждую копию корпоративной информации, где бы она ни находилась и использовалась – на рабочих станциях пользователей, лаптопах и мобильных беспроводных устройствах, в других репозиториях, внутри и снаружи периметра сети.

Например:

- Если документы или почтовые сообщения, являющиеся собственностью компании, запечатаны, то они не только защищены от подделки (никто не имеет права их редактировать), но и, когда приходит время их удалить, каждая их копия может быть эффективно изъята с помощью удаления ключа раскодирования с сервера Oracle IRM. Это является естественным расширением решения Oracle Universal Record Management (универсальное управление записями), которое управляет документами, находящимися в мультивендорных репозиториях, распространяя политику даже дальше, до применения к каждой отдельной копии.
- Если запечатывание применятся к документам в репозитории (таком, как Oracle Universal Content Management), имеющим версии, то Oracle IRM может быть сконфигурирован так, чтобы автоматически изымать доступ к старым версиям, если в репозитории находится более новая версия. Если пользователи локально, вне репозитория сохранили старые версии документов, они не только не получат доступа к старым версиям, но и находящиеся внутри документов ссылки (URL) их приведут к новым версиям, хранящимся в контролируемом репозитории. Своевременное обеспечение пользователей самой новой информацией способно заметно сократить расходы компаниям и государственным агентствам и быть уверенным в более полном соблюдении инструкций и правил.

Как работает управление правами

Oracle Information Rights Management имеет запатентованную архитектуру распределения прав между центральным сервером Oracle IRM и агентами (Oracle IRM Desktop agents), которые должны быть инсталлированы на каждом устройстве, которое создаёт или использует запечатанную информацию.

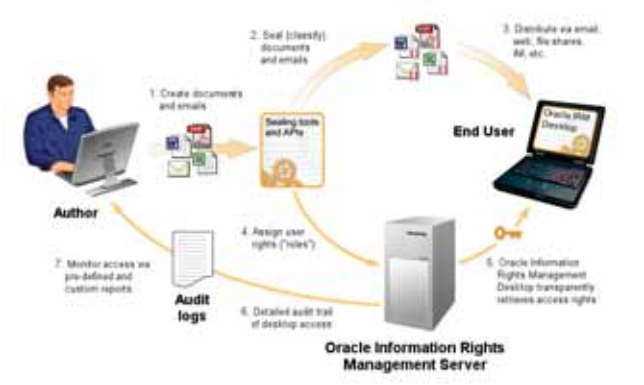

Рисунок 2. Архитектура Oracle Information Rights Management

На рисунке 2 показано, как работает архитектура Oracle IRM (для большей ясности некоторые элементы опущены, например, интеграция между Oracle IRM сервером и корпоративной инфраструктурой по управлению идентификацией и аутентификацией).

1. Авторы продолжают создавать документы и электронные сообщения с помощью существующих приложений, таких как Microsoft Office, Microsoft Outlook, Adobe Reader, Lotus Notes и т.д.
2. Oracle IRM позволяет автоматически или в ручном варианте запечатывать документы на различных стадиях их жизненного цикла с помощью средств, интегрированных в Windows desktop, приложения по созданию документов, клиентские программы электронной почты и общих репозиториях. Запечатывание защищает документы и электронные сообщения с помощью механизмов кодирования и цифровых электронных подписей, вшивая неудаляемые привязки (links) к находящимся в сети серверам Oracle IRM (управляемым организацией, которой принадлежат документы), которые хранят информацию для раскодирования и права доступа к документам.
3. Запечатанные документы и электронные сообщения могут распространятся любым доступным способом (email, web, через файловые сервера и т.д.)
4. Права на запечатанные документы могут быть жёстко привязаны ко времени запечатывания, хотя в сложных корпоративных системах эта функция редко используется ввиду того, что пользователи не хотят использовать слишком сложные механизмы распределения прав. Права сохраняются отдельно от запечатанных документов и почтовых сообщений на сервере Oracle IRM, позволяя менять права в любое удобное время.
5. Для создания и использования документов и электронных сообщений привычными средствами конечные пользователи должны загрузить и инсталлировать универсальный агент, называемый Oracle IRM Desktop. Агент Oracle IRM Desktop имеет небольшой размер, прост в инсталляции и отвечает за аутентификацию пользователей, прозрачным образом запрашивая права с сервера Oracle IRM, защищая и протоколируя работу с запечатанными документами и почтовыми сообщениями, когда они используются встроенными средствами рабочих станций.

Заметим: Запатентованная компанией Oracle распределённая архитектура синхронизации прав доступа и аудита событий между сервером Oracle IRM и клиентом Oracle IRM Desktop обеспечивает возможность пользователям работать off-line, не заботясь о синхронизации.

6. Сервер и агенты Oracle IRM совместно обеспечивают аудит всех попыток обращения к запечатанным документам и электронным письмам (on-line и off-line), всех административных операций, таких как назначение или изъятие прав. Можно управлять степенью детализации аудита, а записи аудита могут храниться в базе данных на сервере Oracle IRM, посланы через очередь сообщений внешним приложениям для обработки или могут экпортироваться в журнальные файлы для дальнейшего импорта в стандартные средства генерации отчётов.
7. Консоль управления Oracle IRM Management Console и Oracle IRM Web Service SDK обеспечивают отчётность на основе запросов с преднастроенными полезными отчётами, такими как «Активность пользователей» или «События по определённому документу», а также и отчёты определяемые пользователем. Средства аудита Oracle IRM открывают беспрецедентные возможности аудита использования (или злоупотребления) корпоративных документов на рабочих станциях пользователей, и только одно это свойство оправдывает инвестиции в Oracle IRM (не говоря о прочих выгодах для обеспечения безопасности).

Ключевые архитектурные отличия от других решений

Два аспекта в архитектуре Oracle Information Rights Management, имеющие чрезвычайно важное значение для корпоративного использования, отличают решение Oracle от продуктов других вендоров:

1. Oracle использует модель прав, основанную на классификации документов, что позволяет присваивать права не отдельным файлам, а наборам. Как результат, необходимо оперировать с меньшим количеством прав. А это, в свою очередь, делает возможным периодическую или автоматическую синхронизацию прав и событий аудита между сервером и агентами Oracle IRM.
2. Автоматическая синхронизация делает возможным полностью прозрачную работу off-line с запечатанной информацией (мобильные пользователи), оставляя в силе централизованное аннулирование или изменение прав.

Конкурирующие решения управляют правами на основе индивидуальных файлов. Для корпоративных объёмов информации это означает слишком большой объём прав для автоматической синхронизации с рабочими станциями. Администраторы таких решений вынуждены выбирать между механизмом кэширования прав (чтобы позволить off-line работу), постоянно находящихся на рабочих станциях, тем самым, жертвуя возможностью изъятия прав, или, всё же, оставляя отмену прав и жертвуя работой off-line. Конкурирующие решения не могут обеспечить одновременно работу off-line и возможность изъятия прав.

Успешное применение системы управления правами

Для того, чтобы система по управлению правами доступа к данным могла быть успешно внедрена в сети гетерогенных серверов и рабочих станций в современных крупных организациях, имеющих партнёров, клиентов, подрядчиков, такое решение должно быть **безопасным**, **удобным** рядовым пользователям и корпоративно **управляемым**

(конечными пользователями, владельцами бизнес-процессов и администраторами).

Заметим: Даже в случае первоначального использования такой системы управления правами доступа для определённого набора приложений и ограниченного количества пользователей, покупателю лучше всего рассматривать применение его для организации в целом (чтобы получить все выгоды от использования решения).

Безопасность

Конечно, не бывает стопроцентно неуязвимой системы защиты против грамотных профессиональных хакеров (особенно действующих изнутри компании). Но Oracle IRM предоставляет механизмы эффективной многоуровневой защиты на основе индустриальных стандартов и лидирующих технологий безопасности. Как результат, это решение очень легко в использовании авторизованными пользователями и очень сложно для компрометации. Элементы многоуровневой модели безопасности включают в себя: постоянный контроль, аутентификацию, кодирование, электронные подписи и механизмы контроля уязвимостей.

Постоянный контроль

Oracle Information Rights Management может контролировать каждый аспект использования запечатанных документов на рабочих станциях пользователей:

- *Кто:* контроль, кто смог и кто не смог открыть документы
- *Что*: контроль доступа к набору (согласно классификации) или к любому конкретному документу
- *Когда:* контроль того, когда доступ начался и закончился с возможностью отмены права доступа в любой момент
- *Где*: предотвращение возможности доступа к критическим документам снаружи сети
- *Как*: контроль того, как именно пользователи работают с документами на своих рабочих станциях (с глубоким контролем открытия, аннотирования, внесения изменений, трассировкой изменений, контролем копирования, отправки на печать, работы с полями и ячейками форм, просмотром табличных формул и т.д.)

Во всех случаях этот постоянный контроль осуществляется на протяжении всего жизненного цикла документов и электронных сообщений вне зависимости от того, где они находятся и используются.

Аутентификация

Oracle Information Rights Management поддерживает следующие три механизма аутентификации:

- Windows аутентификация (для Single SignOn)
- Имя пользователя и пароль (для внешних пользователей)
- Web-аутентификация

Windows аутентификация используется в качестве прозрачной аутентификации при нормальном заходе пользователей в сессию Windows. Аутентификация по имени и паролю встроена в Oracle IRM для поддержки внешних пользователей, когда не нужно требовать захода в Windows-домен. Web-аутентификация означает заход на сервер Oracle IRM основываясь на аутентификации сессии браузера (схема работы web-сервера и

web-браузера). При некоторой доработке Web-аутентификации её можно использовать для интеграции Oracle IRM с любыми системами аутентификациями, такими как RSA SecurID, PKI сертификаты и др.

Кодирование

Oracle Information Rights Management использует алгоритмы кодирования для выполнения функций защиты сообщений от несанкционированного доступа, а именно:

- Запечатывания документов и электронных сообщений. Обычно это повышает размер файла менее чем на 1%.
- Защиты сетевых телекоммуникаций между сервером и агентами Oracle IRM.
- Для защиты прав доступа на агенте Oracle IRM desktop.
- Для работы с контрольными суммами программных компонент Oracle IRM.

В дополнение, Oracle IRM использует другие дополнительные алгоритмы, например запутывание программного кода (software obfuscation).

Tamper–proofing

Кодирование не предотвращает от копирования с экрана, от попыток залезть внутрь программного обеспечения. Поэтому Oracle IRM имеет дополнительные средства для защиты от попыток взлома программного обеспечения:

- Низкоуровневый контроль «лазеек» в приложениях и вызовах функций операционной системы, таких как доступ к виртуальной памяти, видеопамяти или копирования экрана
- Традиционные техники электронных подписей кода, такие как Microsoft Authenticode
- Layered code and interface obfuscation
- Поддержка доверенных часов, а не часов на локальных рабочих станциях
- Незащищённая информация никогда не пишется на диск.

Обновления системы безопасности

В случае появления нарушений безопасности (бреши) надёжная система должна иметь возможности их исправления. Фундаментальным свойством Oracle IRM является то, что агент Oracle IRM Desktop постоянно связывается с серверами Oracle IRM. В функционал этого решения включена дополнительная возможность (в случае необходимости) автоматически загружать и инсталлировать на компьютерах пользователей необходимые обновления безопасности.

Возможности системы

Поддержка гетерогенной инфраструктуры организации

Широкая и глубокая поддержка современных и унаследованных операционных систем и приложений является серьёзным аргументом при внедрении в реальных распределённых гетерогенных системах корпоративного уровня. Важно также, чтобы внедряемые решения работали на самых последних версиях, чтобы при возможных обновлениях функционирование всех систем не прерывалось. Поэтому Oracle поддерживает широкий диапазон последних и устаревших версий приложений и операционных систем Microsoft и других компаний:

- Microsoft Office 2000-2003 (Word, Excel, PowerPoint)
- Adobe Acrobat или Reader 6.0+
- Email: Microsoft Outlook 2000-2003, Lotus Notes 6.5+ и Novell GroupWise 6.5-7.0
- Email: BlackBerry for Exchange and Domino, BES 4.1+
- HTML и XML (Internet Explorer 6.0+)
- .TXT и .RTF документы
- GIF, JPEG и PNG
- TIFF и 2D CAD (требует соответствующих программ-просмотра)

Лёгкая интеграция в существующие бизнес–процессы

Возможность управления корпоративными документами на рабочих станциях пользователей является важным для администраторов бизнес-процессов, но желательно, чтобы влияние на существующие процессы было минимальным. Oracle Information Rights Management имеет несколько ключевых свойств, которые позволяют с лёгкостью интегрировать запечатывание документов в существующие бизнес-процессы:

- Очень небольшой единый пакет инсталлятора агента Oracle IRM требует минимальных административных привилегий
- Конечные пользователи могут создавать, открывать и использовать запечатанные документы с помощью своих привычных приложений
- Создание стандартных электронных сообщений происходит в обычном email-клиенте, а отправка – по кнопке «запечатать и отправить» (вместо «отправить»)
- Правая кнопка мышки позволяет запечатывать, менять печать и создавать запечатанные документы в интерфейсе Windows Explorer
- Осуществляет единый вход (Single SignOn) в NT-домены и автоматический заход для не NT-аутентификации.
- Осуществляет обработку ошибок и исключений (таких как «нет прав») с помощью интегрированной программы самообслуживания.
- Встроенная интеграция полнотекстового индексирования и поиска в запечатанных файлах.

Поддержка off–line работы

Довольно значительная часть работы является мобильной, и есть необходимость использовать запечатанные документы и электронные сообщения в режиме off-line. Oracle Information Rights Management является единственным решением, предлагающим возможность off-line работы объединённой со способностью изъятия доступа к запечатанным документам.

Oracle IRM агент автоматически синхронизирует права конечных пользователей на рабочих станциях без вмешательства самих пользователей (вместо других непрактичных схем, где, например, требуется процесс идентификации требуемых документов до того, как переходить к off-line работе). Для каждой роли Oracle IRM можно сконфигурировать off-line периоды, устанавливая, тем самым, баланс между удобством off-line работы и безопасностью (возможностями быстрого отзыва прав наиболее конфиденциальных документов). Запечатанные документы и электронные письма могут быть созданы и использованы в режиме off-line и операции, такие как открытие и распечатка протоколируются в защищённый буфер для дальнейшей передачи на сервер Oracle IRM. В результате создаётся полный хронологический протокол off-line доступа пользователей к запечатанным документам на удалённых рабочих станциях.

Управляемость

Управление на основе классификаций прав

Уникальный подход компании Oracle по управлению доступом к информации на основе классификации прав позволяет организации легко контролировать доступ к большому количеству документов в терминах существующих бизнес-процессов или уже имеющейся классификации информации (например, по степени секретности – «секретно», «совершенно секретно»), по существующим бизнес-ролям (таким как «рецензент»), по существующим группам пользователей, определённым в каталоге пользователей (например, «менеджеры отдела продаж»).

Диаграмма на рисунке 3 иллюстрирует простоту и удобство управления на основе классификации прав. Восемь файлов были запечатаны с использованием двух предопределённых классов («рабочие документы» и «объявления компании»). Пользователи финансовый директор (CFO), начальник отдела кадров (HR Director) и группа «Все пользователи» (all employees) получили необходимые права на эти классы, что в результате породило четыре разных права доступа на эти восемь документов. Масштабируемость и управляемость системы Oracle IRM проявляются в том, что количество запечатанных документов легко со временем может вырасти от восьми до восьми тысяч, при этом, не изменяя количества прав доступа (всего четыре), потому что привязка идёт на классы, а не на индивидуальные файлы. А так как нет необходимости управления огромным числом прав (как у некоторых конкурентов), данное решение Oracle имеет не имеющие себе равных надёжность и масштабируемость, работая при этом на относительно скромном аппаратном обеспечении.

Oracle IRM поддерживает возможность иметь исключения из общих правил (неизбежные в реальной жизни) для классификации прав доступа, что позволяет администраторам конфигурировать систему на основе индивидуальных пользователей и отдельных файлов. А эта политика использования намного более эффективна, нежели работа с миллионами индивидуальных прав каждого пользователя к каждому файлу. Как только классификация и роли определены в системе, автору документа остаётся только принять решение о том, какой печатью он хочет запечатать свой документ или сообщение электронной почты. Большинству пользователей нет необходимость принимать такие решения, потому что они только читают, рецензируют или меняют уже запечатанные документы и сообщения электронной почты.

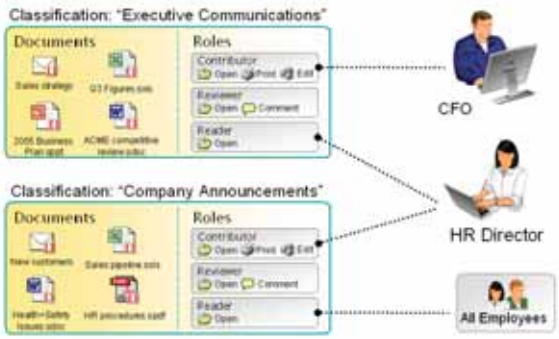

Рисунок 3. Управление на основе классификации ролей

Стандартная модель прав

Для IT-продуктов очень важным является правильное конфигурирование. Особенно важно это для решений типа управления правами. Никто не хочет потерять контроль над закодированной информацией или сделать ненужные барьеры дополнительных аутентификаций и авторизаций между пользователями и той информацией, которая им нужна для выполнения их работы.

Oracle Information Rights Management является единственным решением, построенным в результате пятилетних консультаций, и которое прямо включает в себя наилучшие практики – это называется «стандартной моделью прав Oracle IRM» – лёгкое в использовании web-приложение, включающее в себя предопределённые пользовательские и административные роли, шаблоны классификаций, автоматическое управление пользователями и управлением электронными сообщениями, on-line помощь и учебники администраторов.

Интуитивно понятная стандартная модель прав (Oracle IRM Standard Rights Model) является ключевой составной частью, позволяющей быстро и эффективно адаптировать Oracle IRM прямо на этапе внедрения с доказанной опытом моделью управления правами.

Рисунок 4. Стандартная модель прав

Административная модель на основе ролей

Oracle Information Rights Management отличается от других подобных решений тем, что имеет и ролевую и основанную на классификации административные модели, которые также глубоки и удобны, как и модели управления правами конечных пользователей. Административные операции, такие как создание классификаций безопасности, определение ролей и присваивание прав на основании типов или на основании отдельного документа могут быть выделены и присвоены отдельным пользователям или группам пользователей. Владельцы бизнес-процессов и их помощники легко могут управлять безопасностью их наиболее секретной информации без привлечения IT-администраторов (то есть можно обойтись без дополнительных суперпользователей).

Аудит

Oracle Information Rights Management осуществляет аудит всего on-line и off-line доступа конечных пользователей к запечатанным документам и электронным письмам, а также и все административные операции, такие как присваивание или изъятие прав. Можно настраивать уровень детализации аудита, а записи аудита могут сохраняться в базе данных на сервере Oracle IRM, посланы в качестве сообщений (message queues)

для использования внешними системами мониторинга или экспортированы в журнальные файлы для дальнейшего импорта стандартными генераторами отчётов.

Консоль управления Oracle IRM и Oracle IRM Web Service SDK дают возможность производить отчёты по аудиту на основе запросов. Они имеют предопределённые отчёты типа «Протокол работы пользователя» и «Все операции по данному документу», а также могут использовать отчёты, определяемые пользователем. Аудит Oracle IRM открывает беспрецедентные возможности по контролю использования или злоупотребления корпоративной информацией на рабочих станциях пользователей, и одно это свойство часто заставляет инвестировать средства в это решение (не говоря уже о том, что оно даёт с точки зрения безопасности).

Интеграция с информационной инфраструктурой

Шлюз Oracle IRM Directory Gateway интегрируется с корпоративными LDAP-каталогами, такими как Microsoft Active Directory и Sun ONE Directory Server для синхронизации сервера Oracle IRM с централизованными определениями пользователей и групп. Oracle IRM Directory Gateway также поддерживает расширения и плагины для синхронизации пользователей и групп пользователей с корпоративными базами данных, доменами Windows и другими источниками. Oracle IRM включает в себя также функционально полный и лёгкий в использовании Oracle IRM Web Service SDK для программирования интеграции с дополнительными инфраструктурами, такими как web-приложения. Системы управления содержимым, сканерами фильтрации содержимого и т.д.

Производительность и масштабируемость

Экстенсивное кэширование, присущее патентованной распределённой архитектуре Oracle Information Rights Management, комбинированное с моделью прав на основе классификации (а не на основе отдельных файлов) позволяют избежать сильного сетевого трафика и загрузки сервера Oracle IRM (в отличие от других аналогичных продуктов). Это позволяет достичь дополнительного масштабирования и весьма скромных требований к аппаратной части. Типовая конфигурация Oracle IRM на простом сервере показывает способность обслуживать свыше 50,000 пользователей.

Технологические характеристики и спецификации

Oracle Information Rights Management имеет четыре ключевых компонента:

- **Сервер Oracle IRM Server** – хранит ключи раскодирования и управляет правами пользователей к запечатанным документам и электронным письмам
- **Агент Oracle IRM Desktop** – позволяет авторизованным пользователям создавать и использовать запечатанную информацию в зависимости от прав, полученных с сервера Oracle IRM
- **Консоль управления Oracle IRM Management console** – позволяет администратору управлять всеми аспектами решения Oracle IRM.
- **Oracle IRM Standard Rights Model** – web-приложение, позволяющее бизнес или IT-администраторам создавать новых пользователей, присваивать роли и т.д.

Топология примера внедрения Oracle Information Rights Management

Рисунок 5 иллюстрирует типичную конфигурацию Oracle IRM для корпоративного использования. На одном сервере, обычно расположенном в демилитаризованной зоне, работает серверная часть Oracle IRM и web-приложение Oracle IRM Standard Model. Сервер Oracle IRM использует высоконадёжную базу данных, расположенную в кластере внутри корпоративной сети. Все пользователи используют агент Oracle IRM Desktop, а пользователи с административными правами – ещё и консоль управления Oracle IRM Management Console. Обмен информацией происходит по защищенному каналу, используя 80 порт (рекомендация).

Эту простую, но очень наглядную топологию легко можно масштабировать для работы с очень большим числом пользователей и при высокой нагрузке. В более усложнённых схемах возможно применение основного и запасного сервера Oracle IRM в локальной (приватной) сети, что даёт дополнительную гарантию того, что внешние пользователи не могут получить доступ к информации внутреннего пользования. Сервер Oracle IRM хранит всё своё текущее состояние во внутренней базе данных, механизмы кэширования могут быть отключены, а запасной сервер сконфигурирован для использования в случае сбоя (failover).

Интеграция Oracle Information Rights Management

Хотя в решении Oracle Information Rights Management встроены большинство требуемых функций, но в целях более расширенных возможностей в продукт встроены возможности интеграции с корпоративной инфраструктурой и решениями других компаний.

Oracle IRM Web Services SDK имеет документированные примеры по использованию SOAP/WSDL Web-сервисов (применённых в сервере Oracle IRM), дающие разработчикам доступ к сервисам работы с документами и административным возможностям. Типичными применениями библиотеки Oracle IRM Web Services SDK являются:

- Динамическое «запетатывание» файлов, когда они покидают репозиторий, например, файловые сервера, системы управления содержимым, репозитории общей работы и т.д.
- Временное снятие защиты с файлов для полнотекстового индексирования и поиска, преобразование к другим форматам и т.д.
- Запечатывание и снятие защиты с файлов как часть управления жизненным циклом организации
- Интегрирование Oracle IRM с системами управления идентификацией, например, добавление/удаление пользователей, присваивание ролей и т.д.

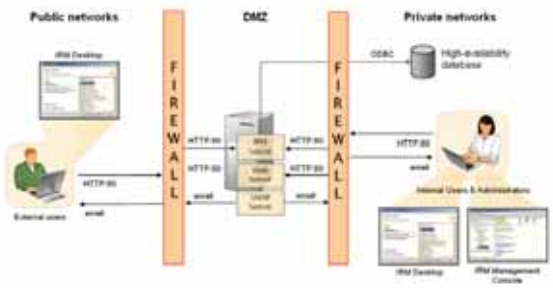

Рисунок 5. Пример топологии использования Oracle IRM

КОРПОРАЦИЯ ORACLE

Oracle Россия
119435, Москва
Саввинская набережная, 15
Тел.: +7 (495) 641 1400
Факс: +7 (495) 641 1414
Email: oracle_ru@oracle.com
Internet: www.oracle.com/ru/

191186, Санкт-Петербург
Невский пр., 25
Тел.: +7 (812) 363 3257
Факс: +7 (812) 363 3258
Email: oracle_ru@oracle.com
Internet: www.oracle.com/ru/

Oracle Украина
04070, Киев
ул. Фроловская, 911
офисный центр «Swiss House»
Тел.: +380 (44) 490 9050
+380 (44) 490 9051
Факс: +380 (44) 490 9052

Oracle Казахстан
480099, Алматы
микрорайон Самал2,
Самал Тауэрс, оф. 97, блок А2, 6-й этаж
Тел.: +7 (727) 258 4748
Факс: +7 (727) 258 4744

Copyright © 2007 Oracle Corporation. Все права защищены.

Данный документ предоставлен исключительно в информационных целях и его содержание может быть изменено без уведомления. Этот документ не гарантирует отсутствие ошибок и не подразумевает никаких гарантий или условий, выраженных явно или подразумеваемых законом, включая косвенные гарантии и условия окупаемости или пригодности для решения конкретной задачи. Мы отказываемся от любой ответственности, связанной с этим документом, и никакие договорные обязательства не могут быть оформлены, прямо или косвенно, на основании данного документа. Этот документ не может быть воспроизведен или передан в любой форме и любыми средствами, электронными или механическими, для любых целей, без нашего письменного разрешения. Oracle, JD Edwards, PeopleSoft и Retek являются зарегистрированными товарными знаками корпорации Oracle и/или входящих в нее компаний. Другие наименования могут быть товарными знаками соответствующих владельцев.

ORACLE