Управление идентификационными данными и правами доступа

ДАНИИЛ МАРКОВ

В условиях консолидации рынка, диверсификации бизнеса и усложнения структуры компаний усложняется и их ИТ-инфраструктура. За последние годы существенно увеличилось число платформ и приложений, используемых компаниями. В большинстве крупных компаний один сотрудник использует в своей работе не менее 3—4 разнородных информационных систем и соответственно такое же количество паролей. В некоторых случаях количество паролей доступа у сотрудника может измеряться двухзначными числами.

В результате этого ИТ-службам приходится управлять совокупностью разрозненных каталогов учетных записей и оперировать сложной системой полномочий доступа. Это приводит к увеличению рутинных операций по администрированию информационных систем, как следствие, к увеличению срока исполнения заявок на предоставление доступа пользователям, к повышению вероятности появления ошибок, связанных с человеческим фактором. Естественным путем компании достигают такого уровня развития ИТ, когда без управления информационной безопасностью им больше жить нельзя.

Эти факторы предопределяют рост интереса к системам управления идентификационными данными и правами доступа пользователя (Identity & Access Management). Такие системы способны решить широкий круг задач: сократить расходы на ИТ-персонал за счет уменьшения количества системных администраторов, обеспечить сохранение конфиденциальной информации с помощью оперативного реагирования на изменения в организационных структурах компаний, реализовать единый жизненный цикл управления учетными записями пользователей для прозрачного контроля доступа к информационным ресурсам компании.

Говоря о системах управления правами доступа, нельзя забывать о том, что соответствие требованиям законодательства и внешних регуляторов (например, закону Сарбейнса — Оксли) во многих случаях является обязательным условием ведения бизнеса. Поэтому часто бизнес, а не CIO или CSO выступает инициаторам проектов по повышению информационной безопасности.

Поскольку все крупные компании испытывают сложности с централизованным управлением учетными данными в корпоративных информационных системах, а с ростом бизнеса эти проблемы лишь усугубляются, целесообразность использования специализированных информационных систем в этой области вызывает все меньше дискуссий. Фокус же этих дискуссий перемещается на обсуждение наиболее оптимальных инструментов управления идентификационными данными и правами доступа пользователя. Одним из таких инструментов является продукт Oracle Identity & Access Management. Тремя фундаментальными принципами Oracle Identity & Access Management являются:

• конфиденциальность — предоставление доступа к информации только уполномоченным лицам, обеспечение надежного контроля доступа к корпоративным информационным ресурсам;

• целостность — защита от несанкционированной модификации данных в корпоративных информационных ресурсах и обеспечение целостности данных в корпоративных системах;

• доступность — эффективное обеспечение уполномоченных пользователей доступом к требуемой информации или требуемым информационным ресурсам компании.

Функциональные возможности Oracle Identity & Access Management позволяют создать монолитный контур безопасности предприятия: закрыть информационные ресурсы от несанкционированного доступа, унифицировать и централизовать политики и сервисы администрирования, повысить уровень сертифицированного доступа к корпоративным приложениям, обеспечить соответствующее мировым стандартам качество аудита, снизить риски информационной безопасности. Использование же трехзвенной архитектуры, в качестве компонентов которой могут быть использованы продукты сторонних производителей, существенно повышает возможности интеграции продукта в корпоративную инфраструктуру.

Среди основных преимуществ Oracle Identity & Access Management:

• гибкая система описания процессов согласования Workflow, которая позволяет настроить систему в соответствии с регламентами управления доступом, принятыми в компании;

• ведение политик, которые позволяют определять правила изменения прав доступа, в том числе и автоматически, при наступлении определенных событий;

• управление политиками паролей в соответствии с корпоративными правилами и автоматическое отслеживание их исполнения в различных информационных системах;

• преднастроенные интерфейсы к ведущим западным приложениям, таким как OEBS, SAP R/3, Microsoft AD, IBM Lotus Notes/Domino, BMC Remedy, PeopleSoft, JD Edwards;

• мощные средства аудита, большой набор предопределенных отчетов — как оперативных, так и исторических, что особенно важно для служб безопасности при расследовании инцидентов по информационной безопасности;

• наличие интеграционных сервисов и API-интерфейса, которые позволяют разрабатывать недостающие коннекторы к информационным системам, реализовывать сложную бизнес-логику.

Среди интересных внедрений на платформе Oracle Identity & Access Management — проект по управлению идентификационными данными пользователей в ОАО “СУЭК”, реализованный компанией IBS Borlas. В крупнейшем в России угольном объединении была создана система для централизованного управления жизненным циклом учетных записей и правами доступа пользователей. Система автоматизирует процессы управления жизненным циклом учетных записей для всех основных информационных систем, используемых ОАО “СУЭК”: Lotus Notes, 1С, Парус, SAP, Microsoft Active Directory, Саперион.

“На основе опыта работы IBS Borlas с Oracle Identity & Access Management нами были разработаны коннекторы к российским системам, таким как 1С, Парус и другим, что существенно облегчило интеграцию этих систем в рамках данного проекта”, — отмечает Роман Пресняков, директор департамента систем корпоративного взаимодействия бизнес-приложений IBS Borlas.

Система, внедренная в ОАО “СУЭК”, автоматически синхронизирует идентификационные данные пользователей в системах, обеспечивает оперативное изменение уровней доступа пользователей.

“В ОАО “СУЭК” была произведена интеграция с HR-модулем SAP, благодаря чему происходит автоматическое отслеживание изменения статуса сотрудника (прием, увольнение, перевод) и на основе этой информации оперативно создаются, блокируются или удаляются учетные записи”, — комментирует Роман Пресняков.

ИТ-специалистам ОАО “СУЭК” доступен широкий спектр отчетов о правах доступа сотрудников за любой период времени. Управление идентификационными данными в ОАО “СУЭК” предусматривает информирование ответственных за информационную безопасность о фактах регистрации учетных записей в обход системы, нарушениях политик управления учетными записями, а также ряд других мер по обеспечению информационной безопасности.

Интересен и опыт по построению системы управления персонализированным доступом в одной из крупных российских металлургических компаний. Здесь были выполнены разработка регламентов информационной безопасности, настройка системы в соответствии с разработанными регламентами. Большая часть работ по внедрению решения Oracle Identity & Access Management выполнялась специалистами IBS Borlas удаленно из московского офиса, что позволило снизить затраты на внедрение и уменьшить время разработки системы.

Следует отметить, что для инструментов Identity & Access Management возможна тесная интеграция с другими составляющими инфраструктуры, в частности достаточно тесная интеграция с системами класса Service Desk. Все это позволяет автоматизировать и ускорить процесс согласования и выполнения заявок на доступ к ресурсам, что весьма важно для крупных компаний. Наличие развитого инструментария в области управления идентификационными данными и правами доступа, не только делает работу сотрудников компаний более удобной и повышает общую информационную безопасность компании, но и является определенным признаком зрелости ИТ-инфраструктуры компании.