

Oracle COREid Access and Identity

Краткий обзор функциональности

Oracle COREid Access and Identity предоставляет комплексный набор сервисов по централизованному управлению идентификацией пользователей и их доступом к различным информационным ресурсам предприятия, в том числе Web-ресурсам и приложениям. Система полностью реализует концепцию защищенного доступа к ресурсам предприятия, известную как концепцию **трех А** (Аутентификация, Авторизация, Аудит), и по оценкам ведущих аналитиков, например, Gartner Group ⁽¹⁾, является лидером на рынке систем управления учетными записями пользователей и их доступом к информационным ресурсам.

Система предоставляет средства, существенно сокращающие расходы на администрирование тысяч и миллионов пользователей (в том числе, например, корпоративного портала), а также на контроль их доступа к информационным ресурсам.

Развитые средства авторизации и аудита действий, как пользователей, так и администраторов системы, позволяют существенно повысить уровень безопасности работы с информационными ресурсами.

Oracle COREid Access and Identity является компонентом прединтегрированного набора продуктов Oracle Fusion Middleware и может работать с широким набором LDAP-каталогов, серверов приложений, Web-серверов, серверов порталов и прикладных приложений, поставляемых ведущими производителями программного обеспечения.

Централизованное управление учетными записями пользователей, политиками доступа и аудита существенно снижает риски несанкционированного доступа с ресурсами, особенно для организаций с большим количеством сотрудников и различных ресурсов.

Система успешно используется в ряде крупных организаций с неоднородной инфраструктурой — British Airways, Coca-Cola, Boeing, General Motors, US Postal Service и др.

Приведем основные характеристики и достоинства системы.

Управление учетными записями пользователей

- Развитые средства проектирования полей учетных записей пользователя, определения групп пользователей и организационной структуры предприятия, а также использование спроектированного интерфейса для создания учетных записей, групп, оргструктуры.
- Широкий набор различных типов групп пользователей: статический, динамический, вложенный, гибридный, на основе подписки. Особенно интересны динамические группы, позволяющие определять группу на основе, например, условий на значения атрибутов учетных записей. Использование групп существенно упрощает администрирование политик доступа.
- Средства автоматизации определения и исполнения процессов (workflow), состоящих как из шагов взаимодействия с различного рода администраторами/менеджерами, так и шагов по получению/передаче данных. Используются для реализации бизнес-процессов утверждения при регистрации пользователей, регистрации их в группах, передачи идентификационных данных во внешние системы (provisioning) и др.
- Средства самообслуживания, позволяющие конечным пользователям самостоятельно создавать свои учетные записи, а также изменять данные в них в рамках предоставленных им полномочий. В частности, это позволяет пользователем менять их пароль. Если необходимо, с изменением поля учетной записи может быть связан workflow, который, например, может запросить согласие менеджера этого сотрудника. Предоставленные средства позволяют организации существенно снизить расходы на администрирование пользователей и их прав доступа, а пользователям — возможность самостоятельно и быстро изменить свои данные.
- Делегирование администрирования, как пользователей, так и политик доступа, которое позволяет создавать многоуровневые иерархии администраторов, каждого со своими полномочиями, обеспечивает распределение нагрузки и высокую адаптивность администрирования к бизнес-структуре организации.

Управление доступом пользователей

- Поддержка аутентификации пользователей на основе: имен и паролей, цифровых сертификатов, смарт-карт, биометрии и др.
- Возможность взаимодействия с внешними системами с целью осуществления расширенной аутентификации и/или авторизации на основе: имен и паролей, цифровых сертификатов, смарт-карт, биометрии и др.
- Поддержка авторизации индивидуальных пользователей и авторизации групп на основе политик авторизации. Развитый аппарат для определения сложных политик доступа.
- Графический интерфейс для определения защищаемых информационных ресурсов, политик доступа, а также средства тестирования определенных политик.
- Авторизация к группе приложений на основе однократной аутентификации (Single Sign-On, SSO). Федеративный SSO.

Oracle COREid Access and Identity

Управление аудитом и отчетность

Система позволяет осуществлять аудит действий, выполняемых средствами управления идентификацией пользователей и их доступом, на основе политик аудита. Возможна запись данных аудита в базу данных, что повышает надежность и защищенность этих данных.

Система поставляется с набором предопределенных отчетов, например, по неуспешным авторизациям (по пользователям или ресурсам), по созданию, активации, деактивации пользователей, по изменению данных в учетных записях.

Заключение

Полное соответствие отраслевым стандартам, открытость и способность функционировать в неоднородной архитектуре позволяет использовать систему в существующей информационной инфраструктуре предприятия с существующими на предприятии серверами порталов, приложениями, реализованными как в трехзвенной архитектуре, так и в архитектуре клиент-сервер. Система имеет средства распространения (provisioning) данных учетных записей и паролей в различные внешние системы.

Функциональность системы может быть доступна для SOA-приложений как Web-сервис.

Система может быть использована совместно с рядом продуктов Oracle, приведенных ниже.

Семейство продуктов Oracle по идентификации пользователей и управлению доступом:

Oracle Internet Directory (OID) – реализация протокола LDAP v.3, опирающаяся на высокую надежность и масштабируемость Oracle Database, используемую для хранения данных каталога. OID активно использует возможности Oracle Database по обработке больших объемов данных, поддержанию одновременной работы большого числа пользователей, высокой готовности на основе Real Application Cluster.

Oracle SSO и DIP – реализация SSO и средств интеграции OID с LDAP-каталогами других вендоров, Oracle HRMS и Oracle Database.

Oracle COREid Access and Identity – система, описанная выше.

Oracle Virtual Directory – система, позволяющая создавать виртуальные LDAP-каталоги на основе LDAP или XML представлений (view) к существующим на предприятии системам хранения учетных записей (различные типы LDAP-каталогов, баз данных и др.) без копирования или синхронизации записей в этих системах хранения.

Oracle COREid Federation – система, обеспечивающая SSO к системам в других доменах через многопротокольный шлюз. Поддерживает все стандарты федеративного доступа, включая SAML, Liberty ID-FF, WS-Federation.

Oracle Web Services Manager – система Аутентификации, Авторизации, Аудита для Web-сервисов, предоставляющая также развитые средства мониторинга исполнения Web-сервисов.

Oracle Xellerate Identity Provisioning – система централизованной идентификации пользователей и распространения (provisioning) данных учетных записей и паролей в различные системы (операционные системы, базы данных, приложения).

Oracle Identity and Access Management Suite – комплект продуктов, включающий: Oracle OID, SSO, DIP, Oracle COREid Access and Identity, COREid Federation, Virtual Directory, Xellerate Identity Provisioning.

Подробную информацию о названных продуктах можно найти на сайте:

<http://www.oracle.com/technology/products/middleware/index.html>

Oracle Россия
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/

Copyright © 2006 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.