

# ORACLE

## Oracle Audit Vault

### Основные преимущества:

- Собирает данные аудита из различных источников, включая Oracle 9i Release 2 и последующие релизы базы данных
- Предоставляет отчеты по безопасности и соответствию стандартам по результатам аудита базы данных
- Уменьшает риски за счет оповещений о подозрительной деятельности
- Контролирует изменения, сделанные привилегированными пользователями
- Защищает данные с Oracle Database Vault
- Поддерживает не-Oracle источники данных на основе C и Java SDK

Oracle Audit Vault позволяет компании решить главную на сегодня проблему по обеспечению безопасности - как защитить данные от внутренней угрозы при помощи контроля за действиями пользователей и соблюдения требований аудита по соответствию стандартам области. Oracle Audit Vault - это мощное решение по аудиту на уровне всей компании, помогающее повысить уровень безопасности и соответствия стандартам и обеспечивающее эффективное управление данными аудита: сбор, мониторинг, контроль, составление отчетов. Oracle Audit Vault предоставляет возможность собирать данные по аудиту и критическим событиям в единый централизованный репозиторий из различных источников, таких как базы данных, серверы приложений, приложения и операционные системы.

### Что такое Oracle Audit Vault?

Соответствие стандартам отрасли и нормативным актам, таким как Sarbanes-Oxley (SOX) в США, Gramm-Leach-Bliley (GLBA), Закон о преемственности страхования и отчетности в сфере здравоохранения (Healthcare Insurance Portability and Accountability Act, HIPAA) в США, стандарт безопасности данных в отрасли платежных карт (PCI, Payment Card Industry), японский закон о безопасности информации (Privacy Law) и директива ЕС о конфиденциальности данных (EU Privacy Directive) требует от компании обеспечения безопасности бизнес-данных и информации о клиентах, сотрудниках и партнерах, а также соответствие этим стандартам пользователей, их действий и информации, с которой они работают.

Существует множество систем, баз данных и приложений, которые создают огромный объем данных журналов аудита. Для того чтобы иметь полную картину о доступе к данным компании, необходимо собирать и вести мониторинг всех этих данных аудита. Аудиторы должны в короткое время проводить анализ данных журналов аудита из разрозненных и гетерогенных систем. Для облегчения этого процесса, необходимо собрать информацию аудита из всех разрозненных источников в единый репозиторий, безопасный, масштабируемый, надежный и в то же время доступный.

Oracle Audit Vault решает эти проблемы безопасности и аудита путем:

- Сбора информации аудита из различных систем компании
- Контроля за изменениями данных информационных систем, проведенными обычными и привилегированными пользователями
- Защиты данных аудита от изменений и несанкционированного доступа

### Сбор, защита и мониторинг данных аудита путем объединения информации

Традиционно безопасности данных аудита уделяется мало внимания, так что привилегированные пользователи системы могут без труда получить к ним доступ. В действительности, данные аудита могут стать мощным средством контроля, если их собрать из различных источников и систематизировать с целью создания отчетности в соответствии со стандартами. Oracle Audit Vault позволяет компаниям собирать данные аудита из различных источников, систематизировать и хранить их в безопасном репозитории, определять состояние данных и создавать необходимые отчеты на основе этой информации.

Oracle Audit Vault предоставляет механизмы для сбора данных аудита, генерируемых Oracle 9i Database Release 2, Oracle 10g Database Release 1 и Oracle 10g Database Release 2. Данные могут поступать из таблиц аудита базы данных Oracle, файлов аудита баз данных, операционных систем и истории операций (Redo log) до/после изменений. Сбор и управление данными аудита из не-Oracle баз данных и приложений производится с помощью инструментария Oracle Audit Vault Software Development Kit.

Так как внешние или внутренние несанкционированные пользователи могут «заметать следы» путем изменения записей журнала аудита, особенно важно защитить и обеспечить безопасность этих данных от изменений и несанкционированного доступа.

# ORACLE

## Oracle Audit Vault

**Защищать, Объединять,  
Определять, Контролировать,  
Управлять, Оповещать и  
Создавать отчеты**

Информационные панели аудита  
Отчеты аудита  
Отчеты пользователей  
Предупреждающие оповещения  
Управление политикой аудита  
Администрирование аудита  
Добыча и анализ данных  
Управление архивом аудита  
Сбор данных аудита

### КОРПОРАЦИЯ ORACLE

Oracle Россия  
123317, Москва  
Краснопресненская набережная, 18,  
БЦ Москва-Сити «Башня на набережной», блок С  
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  
01601, г. Киев,  
Бизнес-центр "Парус"  
ул. Мечникова, 2-а, 16 эт.  
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

Центр по работе с предприятиями  
среднего бизнеса  
Тел.: +7 (495) 981 4780  
Email: oracle\_ru@oracle.com

Copyright © 2008 Oracle Corporation.  
Все права защищены.

Данный документ представлен 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 является зарегистрированным товарным знаком корпорации Oracle и/или входящих в нее компаний. Другие наименования могут быть товарными знаками соответствующих владельцев.

Oracle Audit Vault предоставляет «шлюзовой» репозиторий аудита, единственная цель которого - обеспечивать сохранность и безопасность данных. Доступ к Oracle Audit Vault могут получить только пользователи с новыми, преднастроенными учетными записями: администратор Audit Vault, аналитики аудита, аудитор и архитектор аудита. Все остальные пользователи, включая администратора базы данных (DBA) не имеют доступа к данным аудита.

### Мониторинг и определение изменений, произведенных привилегированными пользователями

Постоянно усложняющийся характер краж информации и внутренних угроз безопасности заставляет бизнес не только повышать защищенность важной информации, но и контролировать доступ к ней со стороны привилегированных пользователей, так как они имеют постоянный и прямой доступ к важной информации. Контроль над этими действиями необходимо осуществлять для выполнения соответствующих стандартов безопасности.

Oracle Audit Vault позволяет проследить, кто, какие операции и с какими данными производил - включая привилегированных пользователей, имеющих прямой доступ к базе данных. Понимание того, кто может изменить, обновить, удалить или просто просмотреть критическую информацию, является важным компонентом в обеспечении безопасности данных и соответствии стандартам. Oracle Audit Vault дает возможность контролировать действия пользователей, создавать отчеты на основе истории изменений данных привилегированными пользователями, определять схемы изменений и даже уровень доступа к данным.

В соответствии с принятой политикой безопасности при помощи Oracle Audit Vault можно определять политики и настройки аудита для источников данных и управлять ими в рамках всей компании. Кроме повышения защищенности данных, централизованное управление политиками и настройками аудита снижает стоимость и сложность самого процесса аудита на всех уровнях бизнеса.

Функционал Oracle Audit Vault также предусматривает возможности по созданию, управлению и настройке системы оповещений о подозрительных действиях, для того, чтобы снизить риск внутренних угроз. Возможности настройки позволяют привязать оповещения к событиям определенной системы или действиям определенного пользователя. Например, оповещение может быть создано, когда привилегированный пользователь создает новую учетную запись без разрешения на это или просматривает важную информацию. Oracle Audit Vault постоянно контролирует доступ ко всей собранной информации и создает оповещения обо всех чрезвычайных событиях или несанкционированных действиях.

### Соответствие стандартам и создание отчетности по безопасности

Веб-интерфейс Oracle Audit Vault дает возможность эффективно собирать данные аудита и информацию о деятельности пользователей, управлять этими данными и информацией, создавать оповещения и отчеты на их основе. Аудиторы и сотрудники безопасности ИТ могут использовать встроенные отчеты, основанные на доступе пользователя к информации и других его действиях, таких как неудачные попытки входа в систему, использование привилегий и изменения структур базы данных. Встроенные возможности позволяют просмотреть такие детали событий аудита, как что, где, когда и кто. Также для контроля над системой оповещений и событиями аудита на всех уровнях бизнеса можно использовать информационные панели Oracle Audit Vault.

\* Сбор данных производится с помощью Oracle Audit Vault SDK, предоставляемого в рамках решений партнеров или следующего релиза продукта.

Июнь 2006, версия 1

Данная информация представляет основные возможности продукта. Все описания предоставлены исключительно с информационной целью и не могут быть использованы в контрактах и договорах.

ORACLE®