С И С Т Е М А

аудита обращений к базам данных

Meridian DB Patrol

2016

Изменения

Дата	Изменения	Автор
16.11.2015	Создание документа	Саенко Сергей
29.02.2016	Актуализация	Саенко Сергей
28.03.2016	Актуализация	Саенко Сергей

Назначение системы

Система **Meridian DB Patrol** предназначена для дополнительной защиты информации в системах управления базами данных (СУБД) поверх штатных средств разграничения доступа.

Аннотация

Система **Meridian DB Patrol** осуществляет пассивный и активный аудит сетевого и локального доступа к СУБД Oracle и MSSQLSERVER в целях мониторинга действий пользователей и защиту хранимой в СУБД конфиденциальной информации. Система протоколирует все обращения к СУБД на основе заданных критериев политик безопасности, протоколы сохраняются во внутреннем аналитическом хранилище и доступны для последующего анализа службами информационной безопасности предприятий.

Оглавление

Функциональные возможности системы

Для данных, хранящихся в СУБД, система **Meridian DB Patrol** обеспечивает:

I. Аудит работы с данными в многозвенной архитектуре в режиме реального времени

Система протоколирует все сетевые обращения пользователей к базе данных (БД) как в двухзвенной (прямые обращения с клиентских рабочих мест), так и в многозвенной архитектуре (обращения через сервера приложений). В протокол аудита попадают:

- Конструкции языка SQL:
  1. Обращение к данным (SELECT, INSERT, MERGE, UPDATE, DELETE), включая диалекты и модификации языка SQL от ORACLE и MSSQLSERVER, вошедшие в стандарт SQL 99 и 2006 (конструкции с подзапросами, подсказками оптимизатору, рекурсивные и иерархические конструкции, аналитические конструкции и т.п.)
  2. Изменение схемы БД (ALTER, CREATE, DROP, TRUNCATE)
  3. Разграничение доступа к данным (CREATE USER, ALTER USER, DROP USER, ALTER LOGIN, DROP LOGIN, CREATE LOGIN, GRANT, REVOKE)
  4. Аутентификация пользователей (успешная/неуспешная)
  5. Управление характеристиками процесса модификации данных, параметрами чтения/записи и уровнем изоляции транзакции (SET [LOCAL]-TRANSACTION)
  6. Управление аудитом и анализом статистики (ANALYZE, AUDIT)
  7. Управление ассоциациями (ASSOCIATE STATISTICS)
  8. Изменение типов данных и объектных типов (CREATE TYPE, CREATE OR REPLACE TYPE, ALTER TYPE, DROP TYPE)
- Конструкции языка PL\SQL (Oracle) и языка T-SQL (MS SQLSERVER) (создание, изменение, выполнение анонимных блоков, процедур, функций, методов объектных типов и т.п.);
- Значения переменных параметризованных запросов

II. Контроль работы привилегированных пользователей

Система может функционировать независимо от IT департамента и может полностью контролироваться службой безопасности. В состав решения входят локальный агент, который отслеживает все локальные обращения к базе данных. Это не дает скрыть свою активность даже администратору БД.

III. Режим активного аудита

Система может функционировать в режиме блокировки нежелательных действий пользователей как сетевой экран.

IV. Формирование отчетности для обеспечения соблюдения требований

Система имеет в своем составе рабочее место офицера безопасности, которое позволяет в удобном графическом интерфейсе осуществлять настройку правил и политик протоколирования и формировать отчеты по безопасности.

V. Контроль прав доступа

Система позволяет обнаруживать факты изменения прав доступа на объекты базы данных.

VI. Обнаружение тематической активности при обращении к конфиденциальным данным

Система позволяет настроить шаблоны аудита по ключевым словам в целях обнаружения активности по определенной тематике в общей массе конфиденциальной информации. Например, можно

выявить активность запросов по определенному лицу, организации, номерам телефонов и иным атрибутам конфиденциальной информации, которые хранятся в базе данных.

VII. Строгая поддержка сетевых протоколов обмена данными СУБД.

Система поддерживает протоколы СУБД Oracle версий 9i,10g,11g,12c.

Система осуществляет разбор обращений к СУБД MS SQLSERVER в строгом соответствии со спецификацией MS TDS - прикладного протокола взаимодействия клиентских приложений с СУБД. Поддерживаются версии протоколов, используемые в СУБД MS SQLSERVER 2008 и выше.

Архитектура системы

Система **Meridian DB Patrol** состоит из следующих основных элементов:

I. Анализатор сетевого трафика — съёмник (c++ приложение)

Съёмник обеспечивает разбор и приведение к единому формату событий из протокола доступа к СУБД. Трафик копируется с точек концентрации на съемник с помощью программных (Cisco SPAN) или аппаратных (Network TAP) технологий.

II. Локальный агент (c++ приложение)

Локальный агент представляет собой программное обеспечение, устанавливаемое на сервер СУБД и осуществляющее протоколирование локальных обращений к СУБД.

III. Подсистема хранения и анализа данных аудита (java-приложение + СУБД PostgreSQL)

Система хранения и обработки данных включает в себя СУБД PostgreSQL для хранения и приложение для обработки результатов анализа трафика

IV. АРМ инженера по безопасности (web приложение)

Система имеет в своем составе приложение - автоматизированное рабочее место (АРМ), которое предоставляет инженеру по безопасности Web интерфейс для работы с системой.

Принципиальная архитектура системы **Meridian DB Patrol** приведена на рисунке 1.

В зависимости от специфики конкретной инсталляции анализатор трафика и система хранения данных аудита могут быть объединены на одном физическом сервере. Также система допускает распределенную архитектуру, при которой данные с нескольких съемников обрабатываются одним приложением.

В качестве внутреннего хранилища **Meridian DB Patrol** используется СУБД PostgreSQL. Java-приложение подсистемы хранения и анализа данных аудита обладает развитым API. Это позволяет заказчику при желании прозрачно встроить анализ результатов аудита **Meridian DB Patrol** в собственные корпоративные системы аудита и мониторинга безопасности.

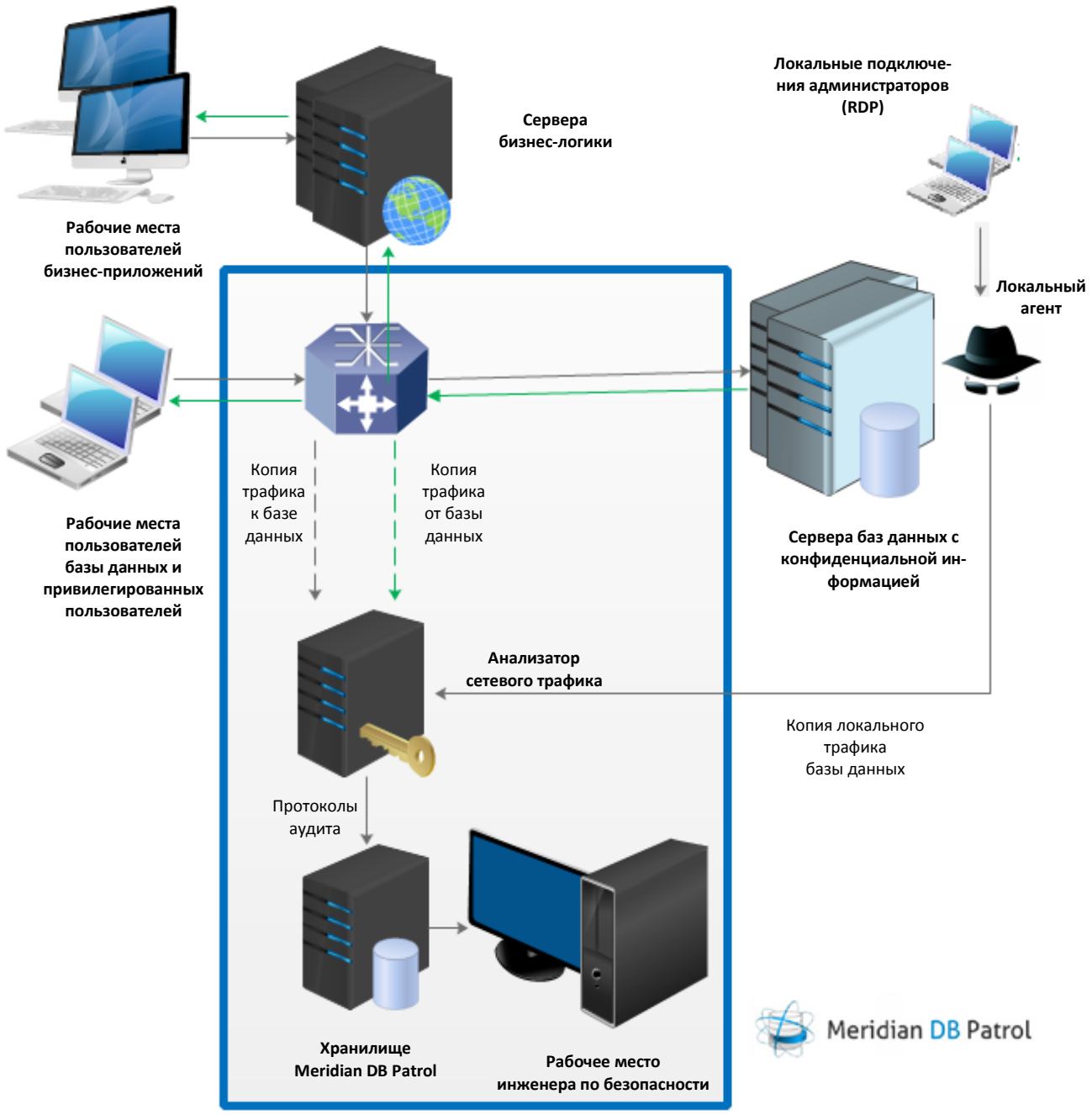

Рисунок 1. Архитектура системы **Meridian DB Patrol**

Система предоставляет пользователю удобный web-интерфейс, позволяющий создавать заявки на получение данных, просматривать результаты в web и выгружать отчеты аудита в pdf и xls, управлять пользователями и многое другое.

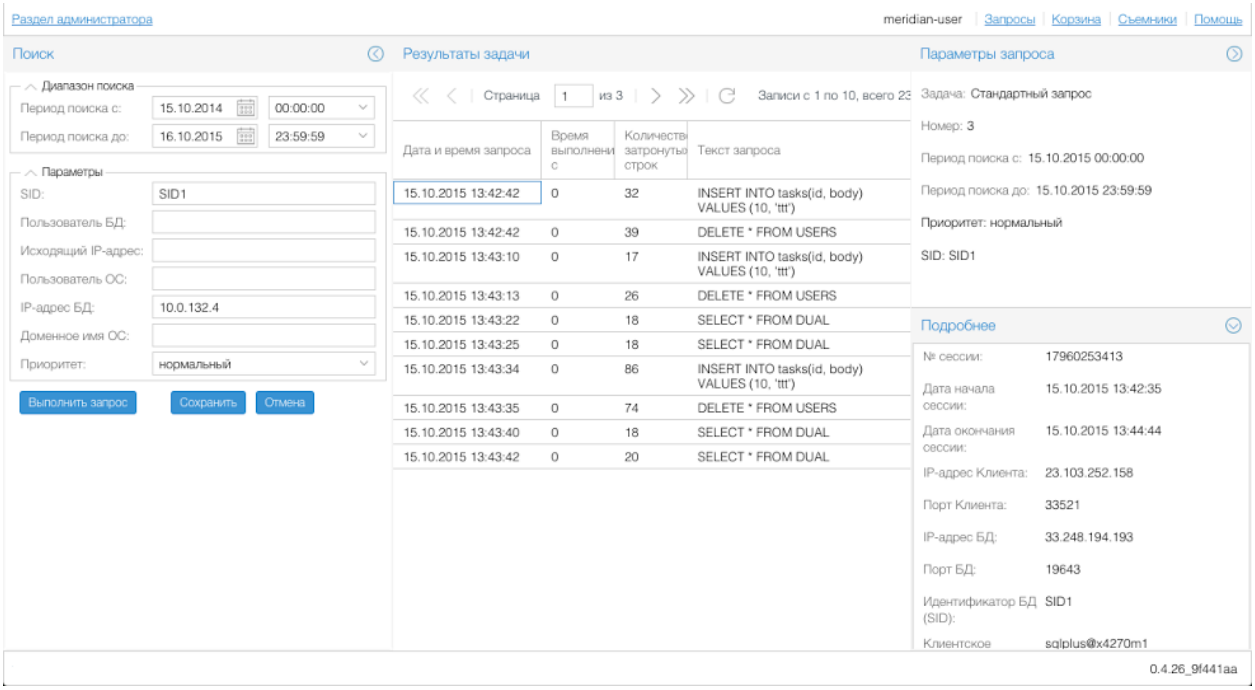

Рисунок 2. Пример интерфейса АРМ инженера по безопасности **Meridian DB Patrol**

Состав информации, накапливаемой в системе Meridian DB Patrol

- Время выполнения запроса
- Доменное имя компьютера клиента
- Доменное имя сервера БД
- SID БД (Oracle)
- Имя схемы БД
- Локальное имя пользователя клиента
- Приложение, выступающее в роли клиента
- Статус аутентификации
- Тип протокола сервера БД
- IP адрес клиента
- Порт клиента
- IP адрес БД
- Порт БД
- Полный текст SQL выражения (PL/SQL-блока, T-SQL-блока)
- Перечень затронутых объектов БД как результат синтаксического разбора запроса (участвующие в SQL-выражении объекты - таблицы, представления, синонимы, процедуры, функции, типы; для табличных типов – перечень полей)
- Переданные в запрос, процедуру или функцию значения параметров (bind-переменных)
- Количество затронутых записей (выбранных записей в случае выборки данных, измененных в случае DML операции)
- Код ошибки (в случае ее возникновения при выполнении запроса)
- Тип запроса
- Признак наличия ключевых слов

Средства обеспечения надежности системы

Система может работать автономно в режиме 24x7x365 и обладает следующими средствами диагностики и обеспечения надежности:

I. Модуль самодиагностики анализатора сетевого трафика

Съемник имеет модуль самодиагностики. Доступна следующая статистика:

- скорость приема данных (сетевых пакетов в единицу времени, байт в единицу времени);
- суммарное число принятых пакетов за период времени;
- суммарное число потерянных пакетов за период времени;
- скорость передачи данных в хранилище;
- объем свободной памяти на момент времени;
- среднее количество сессий в единицу времени.

II. Модуль самодиагностики подсистемы хранения

Доступна следующая статистика:

- скорость загрузки данных в хранилище;
- суммарный объем хранилища;
- объём свободного места хранилища;
- количество одновременных сессий;
- топ отчетов, выполняющихся длительное время;
- текущая глубина хранения.

III. Режим автоматического перезапуска съемников после падения

Поддерживается режим автоматического перезапуска съемников после аварийного падения с фиксацией ошибок в локальном журнале съемника.

IV. Система резервного копирования и восстановления

Поддерживается резервное копирование и репликация журналов аудита средствами PostgreSQL.

V. Режим ротации данных

Хранилищем поддерживается режим автоматической ротации данных при заданной глубине хранения.

Средства защиты системы

Система поддерживает парольный доступ, протоколирование действий пользователей с системой, шифрование обращений от съемников и web-приложения к внутреннему хранилищу системы.

Технические характеристики и ограничения производительности

Ниже приведены основные нагрузочные показатели, при которых была протестирована стабильная работа системы. Реально система может работать и при большей нагрузке, однако это не проверялось тестами.

Показатель	Значение
Трафик в мегабитах в секунду на один съемник	2000 (2 * Ethernet 1000BaseT)

Число съемников	2
Количество запросов в секунду на один съемник	3000
Количество одновременных сессий Клиент-БД на один съемник	20000
Объем данных, загружаемых в подсистему хранения в сутки	50 гигабайт
Общий объем хранимых данных	4 терабайта
Количество одновременно работающих с системой пользователей (инженеров по безопасности), сессий	30
ОС для съёмников-локальных агентов	Linux, Windows
ОС для съемников и хранилища	Linux
ОС для АРМ инженера по безопасности	Linux, Windows, OS X

Ограничения функциональности

- поддерживаются только СУБД Oracle и MS SQLSERVER, частично поддерживается SAS. В ближайшей перспективе планируется поддержка Teradata, MySQL, PostgreSQL;