УДК 004-658

Я.І. Корнага, Н.П. Корнага, Є.Б. Максимова

МОДЕЛЬ МОНІТОРИНГУ ПОДІЙ РОЗПОДІЛЕНИХ БАЗ ДАНИХ НА ОСНОВІ СЕНСОРІВ ПОДІЙ

Анотація: Запропоновано модифікований метод моніторингу в різнорідних розподілених базах даних. Проведено експериментальне дослідження параметрів моніторингу та швидкості обробки даних на сервері моніторингу подій. Проведене порівняння швидкості обробки даних за допомогою файлів та таблиць баз даних.

Ключові слова: моніторинг подій, розподілені бази даних, швидкість обробки.

Вступ

В сучасних різнорідних розподілених СУБД та пошукових системах використовуються різні методи та засоби моніторингу, які дозволяють проводити керування базами даних та налаштовувати їх під відповідні вимоги систем. Механізми, що позволяють налаштовувати параметри роботи бази даних та управляти її роботою потребують приведення до єдиного формату обробки даних [1,2]. Методи обробки подій, що використовуються не завжди в повній мірі висвітлюють вплив даних подій на конкретні умови роботи бази даних [3,4,5].

Постановка задачі

Потрібно створити новий метод моніторингу, який дозволить уніфікувати обробку подій різнорідних розподілених баз даних та за допомогою додаткового сервера пришвидшить їх обробку, а також, дасть можливість усувати виникненні загрози шляхом автоматичного втручання або за допомогою адміністратора.

Модель моніторингу подій розподілених баз даних на основі сенсорів подій

Класична модель моніторингу будується на основі алгоритму найбільших статистичних аномалій (АНСА), тобто формуванні вектора Бернулі, який і обробляється сервером моніторингу. Тобто, формується вектор $\overline{X} = \{x_1, x_2, \ldots, x_n\}$, який порівнюється з пороговим вектором та передається на сервер обробки моніторингу, який приймає рішення щодо тієї чи іншої події.[6] Елементи вектора Бернулі включають в себе тільки параметри подій, але не включають вплив події на той чи інший елемент системи. Тому потрібно створити систему моніторингу подій, яка б дозволяла обробляти не тільки події, а і їх розподіл по відповідним властивостям БД та СУБД.

 ISSN 1560-8956

Модель моніторингу подій розподілених баз даних на основі сенсорів подій:

I. Збір подій моніторингу.

1. На кожну базу даних з розподіленої системи будуємо сенсори подій на основі тригерів.

2. Для кожної множини подій $\overline{E_i} = \{e_1, e_2, \ldots, e_n\}$, які збирають сенсорами подій, будується порогова матриця по можливим наслідкам кожної події з множини $\overline{C_i} = \{c_1, c_2, \ldots, c_m\}$.

3. Сенсори подій проводять збір матриці подій $S_i = \overline{E}_i \times \overline{C}_i$ з простору S та передають їх на сервер моніторингу подій.

II. Метод обробки подій моніторингу на сервері моніторингу подій.

1. Після передачі матриці подій на сервер моніторингу подій проводяться операції різниці між отриманою матрицею S_i та відповідною пороговою матрицею S_0, тобто $B_i = S_i - S_0$.

2. Проводиться формування експертних оцінок, тобто формування вектору $\overline{W}_i = \{w_1, w_2, \ldots, w_m\}$.

3. Після отримання вектору експертних оцінок матриця B_i перемножається на вектор експертних оцінок $\overline{W}_i$ відповідно, $\overline{Z}_i = B_i \times \overline{W}_i$.

3. Отримані результати оцінюємо за допомогою функції R визначення від'ємних значень в векторах, яка формує вектор відповіді $\overline{F}_i = \{f_1, f_2, \ldots, f_n\}$ в який записується результат обробки події.

$$\overline{F} = R(\overline{Z_i}) = R(B_i \times \overline{W}_i) = R((S_i - S_0) \times \overline{W}_i)$$

III. Обробка відповіді серверу моніторингу подій.

1. Вектор $\overline{F}_i = \{f_1, f_2, \ldots, f_m\}$ передається в модуль контролю подій.

2. В модулі контролю подій вразі присутності подій, які можуть спричинити негативні наслідки для баз даних розподіленої системи генерується рішення про застосування тих чи інших мір по нейтралізації негативних наслідків.

3. Вразі виникнення нештатних ситуацій модуль контролю подій передає сигнал через блок формування попередження адміністратору серверу моніторингу подій.

Загальна архітектура засобів моніторингу подій розподілених баз даних на основі сенсорів подій

Розроблена система моніторингу подій автоматично ідентифікує всі події, що відбуваються в розподілених базах даних. В процесі роботи сенсор подій прикріплюється до тимчасово-виділеної пам'яті (SGA у разі Oracle) і циклічно запускає опитування з моніторингу подій шляхом вибірки даних з пам'яті з певною частотою. На кожному циклі сенсор виконує аналіз активних в даний момент процесів у кожній сесії в базі даних і визначає за допомогою

встановлених адміністратором правил події. Повідомлення про події відправляються на сервер моніторингу подій для їх подальшого аналізу і генерації відповідних повідомлень.

На рисунку 1 зображено схему, яка була створена на основі розробленої моделі.

Рис. 1 – Архітектура моделі моніторингу подій на основі сенсора подій

Система моніторингу подій (детальне зображення архітектури сенсора та серверу подій на рисунку 2) також може примусово достроково припиняти сесії роботи в разі певних несанкціонованих подій з боку користувачів. З іншого боку, для його роботи потрібна незначні обчислювальні ресурси бази даних і він практично не впливає на операції обробки запитів. Упереджувальна функція сенсора може бути реалізована з використанням DDL-тригерів, які вибірково затримують виконання команд DDL і DCL на короткі проміжки часу (кілька мілісекунд), що дозволяє сенсору подій своєчасно реагувати на небезпечні дії.

Виділений сервер моніторингу подій в запропонованій системі моніторингу подій може керувати кількома сенсорами подій з різних розподілених баз даних, а також він підтримує функцію масштабування числа сенсорів подій. Сервер досить просто інтегрується в структуру системи моніторингу СУБД, що дозволяє підвищити ефективність загального управління надійності обробки даних в розподілених базах даних.

Структура пропонованої системи також забезпечує розподіл прав і повноважень між суб'єктами, що є одною з основних вимог

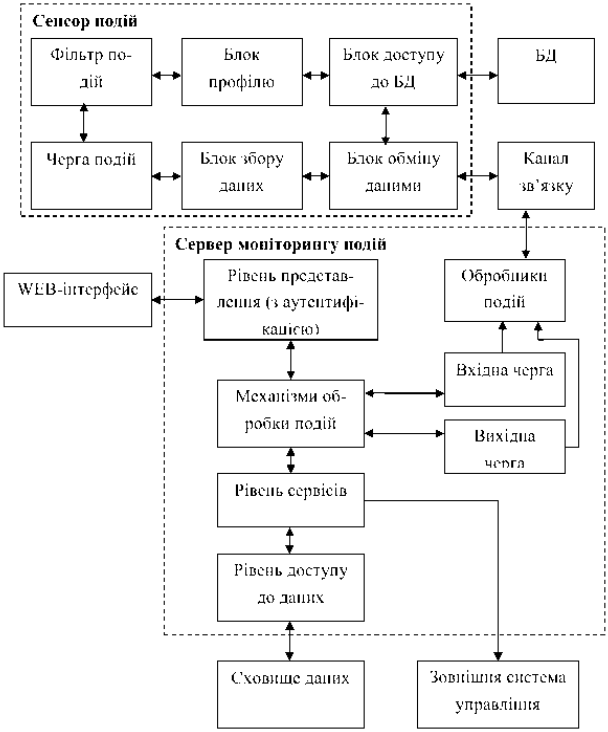

Рис. 2 – Архітектура сенсору подій та серверу моніторингу подій

до системи найденої обробки даних. Адміністратор цієї системи є персоною, що визначає правила політики надійності та безпеки і отримує повідомлення про інциденти через блок формування попередження. Запропонована система дозволяє, з одного боку, забезпечити необхідний рівень надійності обробки даних в розподілених базах даних, а з іншого - безперервне виконання обробки запитів.

Результати досліджень системи моніторингу подій розподілених баз даних

Для проведення дослідження параметрів системи моніторингу подій в розподілених базах даних була вироблена методика, яка дозволяє оцінювати ефективність функціонування серверу моніторингу подій на основі сенсорів подій.

Операції в базах даних можна класифікувати за наступними ознаками:

1. Дозволені.

2. Не дозволені.

Нехай G – кількість можливих подій в базі даних, K – множина нормально відпрацьованих подій в БД. Позначимо: $i \in G$ – множина подій, які не були виявлені системами моніторингу подій, $o \in K$ – множина нормально відпрацьованих подій, які були невірно ідентифіковані системою моніторингу подій елементи як порушення надійності.

Ймовірність коректного виявлення подій розраховується як:

$$P_i = 1 - \frac{i}{G}.$$

Ймовірність невірних ідентифікацій нормально відпрацьованих подій розраховується як:

$$P_k = 1 - \frac{i}{G - i + k},$$

де $G - i + k$ – кількість несанкціонованих подій, які були виявлені системою моніторингу подій.

При цьому ймовірність коректного виявлення несанкціонованих подій системою моніторингу подій розраховується як:

$$P = 1 - \max\{P_i, P_k\} = 1 - \max\{\frac{i}{G}, \frac{k}{G - i + k}\}$$

Отриманий показник використовується для комплексної оцінки ефективності функціонування системи моніторингу подій в розподілених базах даних.

Ймовірність коректної роботи серверу моніторингу подій визначається як:

$$P_{=}1 - \max\{P_I, P_{II}\},$$

де P_I – ймовірність помилки I роду (відсутність реакції на подію), P_{II}– ймовірність помилки II роду (помилкове спрацювання).

Рис. 3 – Архітектура сенсору подій та серверу моніторингу подій

Експериментальні дослідження, як показано на рисунку 3, проводилися в двох напрямках:

1. Виявленні кількості спроб інцидентів.
2. Сумарна кількість помилок I та II роду в системі моніторингу подій.

Висновки

Запропоновано спеціалізований механізм реалізації моніторингу подій баз даних, за допомогою якого виконується комплексний моніторинг усіх дій з базою даних і забезпечується захист від несанкціонованих дій легальних користувачів. Також даний механізм дозволяє виконати детальний моніторинг транзакцій, запитів, об'єктів і збережених процедур бази даних з повідомленнями про інциденти в режимі реального часу і попередженням вторгнень. Крім того, запропонований механізм дозволяє провести відстеження нових виявлених вразливих місць бази даних і оперативно усунути ці уразливості, що важливо в практичних застосуваннях.

Літературні джерела

1. Marcus Hirt, Marcus Lagergren Oracle JRockit: The Definitive Guide / Packt Publishing, 2010. – 588 c.
2. Teo Lachev Applied Microsoft SQL Server 2008 Reporting Services / Prologika Press, 2008. – 768
3. Горєв А., Ахаян Р., Макашарипов С. Ефективна робота із СУБД / Питер Кому, 2006. – 704 с.
4. Джен Л. Харрингтон Проектування реляционних баз даних / Лорі, 2006. – 230 с.
5. Коннор Мак Дональд Oracle. Практичні рішення / ДиаСофтЮП, 2006. – 560 с.
6. Мухін В.Є., Корнага Я.І. Механізми підвищення ефективності процедури моніторингу безпеки в розподілених базах даних / Вісник Національного технічного університету "Харківський політехнічний інститут". Збірник наукових праць. Серія: Інформатика та моделювання. / Харків: НТУ "ХПІ", 2012. – № 38., С 128–135.

Отримано 28.03.2014 р.