УДК 004.04

В.Є. МУХІН, канд. техн. наук, доц., НТУУ "КПІ", Київ,
Я.І. КОРНАГА, ст. викл., НТУУ "КПІ", Київ

МЕХАНІЗМИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПРОЦЕДУРИ МОНІТОРИНГУ БЕЗПЕКИ В РОЗПОДІЛЕНИХ БАЗАХ ДАНИХ

Розглянуто засоби підтримки безпечної обробки даних в розподілених базах даних. Визначено основні компоненти системи управлінням моніторингу серверу безпеки даних. Запропоновано засоби моніторингу безпеки з прискореною обробкою даних. Для аналізу ефективності цих засобів проведені експериментальні дослідження часу пошуку і вибірки даних з моніторингу безпеки. Іл.: 3. Табл.: 1. Бібліогр.: 10 назв.

Ключові слова: бази даних, сервер безпеки, моніторинг, пошук і вибірка даних.

Постановка проблеми. Системи управління базами даних (СУБД), в особливості розподілені реляційні СУБД, є домінуючим інструментом зберігання великих масивів інформації. Розвинені інформаційні програми покладаються не на файлові структури операційних систем, а на багатокористувацькі СУБД, реалізовані за технологією клієнт-сервер. В зв'язку з цим забезпечення інформаційної безпеки СУБД, і, в першу чергу, їх серверних компонентів, набуває вирішального значення для безпеки організації в цілому.

Для СУБД важливі всі три основні аспекти інформаційної безпеки – конфіденційність, цілісність та доступність. Таким чином, виникає ряд проблем, пов'язаних з необхідністю забезпечення захисту потоків даних, якими обмінюються в клієнт-серверних системах. Побудова механізмів моніторингу та захисту даних на сервері СУБД є актуальною проблемою.

Аналіз літератури. На рис. 1 представлена узагальнена схема засобів підтримки безпечної обробки даних в розподілених базах даних між клієнтом та сервером [1, 2, 3]. Вона включає в себе наступні елементи:

– комп'ютерна мережа – середовище передачі даних;

– сервер бази даних;

– база даних;

– робоча станція клієнта, з якої формуються запити на сервер бази даних;

– сервер безпеки даних, в склад якого входять блоки аутентифікації, розмежування доступу до даних, шифрування та управління моніторингом [3, 4, 5].

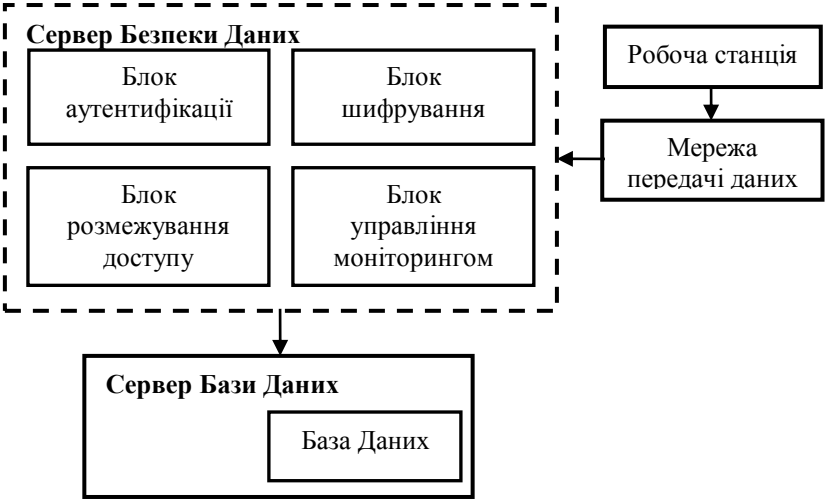

Рис. 1. Засоби підтримки безпечної обробки даних в розподілених базах даних

Клієнт в даній моделі в залежності від поставленої задачі виконує запит до бази даних, який через комп'ютерну мережу незалежно від її типу (локальна, місцева, регіональна, глобальна) попадає на сервер захисту даних [6, 7, 8].

Сервер безпеки даних складається з чотирьох блоків, які відповідають за свій напрямок безпеки.

Перший блок виконує внутрішню аутентифікацію, що проводиться засобами СУБД та зовнішню, яка проводиться засобами операційної системи. Процедуру аутентифікації реалізується шляхом перевірки ідентифікатора користувача та його паролю в залежності від розділу БД до якого він звертається.

Другим блоком сервера безпеки даних є використання механізму розмежування доступу. В клієнт-серверних системах зазвичай використовуються три моделі: дискреційна, мандатна та рольова. Перша та друга моделі використовуються для побудови захисту СУБД традиційно, а от рольова модель розроблена порівняно недавно, вона є більш складною та базується на принципах, що закладені як в дискреційній так і в мандатній моделях.

Третім блоком є блок шифрування даних. В СУБД дані шифруються прозорим та непрозорим способом, кожен з яких має свої переваги та недоліки. Для шифрування зазвичай використовуються алгоритми

шифрування, зокрема: алгоритми групи AES, RSA. Шифрування запитів можна проводити як на рівні самої ОС так і в СУБД.

Четвертим блоком серверу безпеки даних є блок управління моніторингом. Важливим є фактор оперативного реагування на загрози, який пов'язаний з тим, що процедура моніторингу проводиться за накопленими статистичними даними на протязі певного періоду часу. З іншого боку цього недостатньо для підтримки комплексного захисту СУБД, тому потрібна розробка засобів моніторингу, які дозволять проаналізувати всі запити клієнтів-робочих станцій на сервер даних з точки зору ймовірності реалізації несанкціонованого доступу, про що сигналізується через внутрішні та зовнішні системи повідомлень адміністратора.

Актуальним питанням є механізм динамічного моніторингу, який являє собою процес оперативного оцінювання дій суб'єктів (клієнтів) в контексті їх небезпеки з точки зору реалізації несанкціонованого доступу. Визначимо інтервал ΔT – період комплексної оцінки дій суб'єктів на основі аналізу даних по моніторингу безпеки. При відносно великому значенню ΔT моніторинг фактично стає статичним, тобто, на протязі періоду ΔT дії суб'єктів не оцінюються з точки зору ймовірності реалізації несанкціонованого доступу і відповідно істотно зростає ймовірність загроз безпеці процесу обробки даних.

Відомо, що при проведенні моніторингу безпеки розподілених баз даних, особливо таких, які включають в себе значне число записів (понад 1 мільйон екземплярів), розміщених розподілено, виникає проблема оперативної обробки досить великого обсягу даних щодо подій моніторингу. Таким чином, потрібна розробка механізму динамічної обробки даних з моніторингу, який забезпечить оперативне відстеження потенційних вторгнень і атак на базу даних.

Мета статті. Розробити систему моніторингу безпеки з прискореною обробкою даних та експериментально дослідити її ефективність.

Система моніторингу безпеки з прискореною обробкою даних. Пропонується система моніторингу безпеки розподілених баз даних, що підтримує прискорену обробку даних з моніторингу, яка включає п'ять основних блоків: блок спеціальних механізмів збору даних з моніторингу; блок механізмів активації процесу моніторингу; блок перетворення, що виконує перетворення подій моніторингу в дані формату Oracle; блок накопичення даних щодо подій моніторингу та їх зберігання в базі даних, а також блок обробки даних з моніторингу. Структура даної системи наведена на рис. 2.

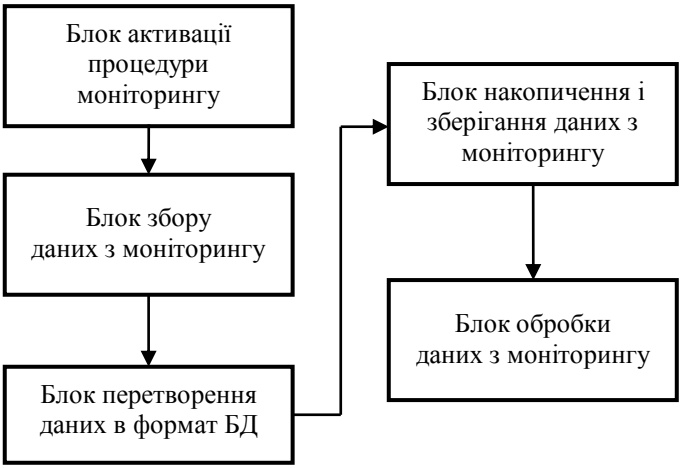

Рис. 2. Основні блоки системи моніторингу безпеки розподілених баз даних

Розглянемо детальніше особливості реалізації представлених вище блоків. Принципово новим елементом є блок перетворення даних з моніторингу в формат бази даних. В загальному випадку цей блок відсутній і дані накопичуються в єдиному файлі. Зокрема, в процесі моніторингу формується вектор критичних подій $X = \{x_1, x_2, x_i, ..., x_n\}$, пов'язаних з подіями порушення безпеки, надалі цей вектор обробляється за певним алгоритмом. Зокрема, в якості аргументів x_i – виступають наступні фактори, що відслідковуються:

x_1 – число спроб звернень до певних даних бази даних;

x_2 – число спроб модифікації певних даних;

x_3 – кількість спроб входу в базу під певним ім'ям і т.д.

Для реалізації ефективної системи моніторингу безпеки дії кожного із суб'єктів необхідно оцінювати за результатами декількох (в загальному випадку, не менш 10 –15) сеансів його роботи з базою даних. У тому випадку, якщо БД є розподіленою, до неї звертається ряд суб'єктів, по кожному з яких необхідно зібрати відповідну інформацію в форматі вектора *X*. На практиці, з огляду на особливості функціонування розподілених систем, число записів щодо подій моніторингу в них виявляється значним, причому самі ці записи формуються в порядку взаємодії суб'єкта з БД, тим самим дані про події безпеки по одному суб'єкту виявляються розподіленими практично по всьому файлу записів.

В процесі обробки файлу записів по вектору моніторингу *X* фактично виконується пошук, вибір даних і кортежів даних за заданим шаблоном. З ростом розміру файлу записів щодо подій моніторингу

безпеки ускладнюється і уповільнюється процедура пошуку та обробки даних, що характерно при зборі статистики для розподілених баз даних, які містять значний обсяг даних. Затримки в процедурі аналізу даних з моніторингу безпеки можуть привести до виникнення ситуацій пропуску значної кількості атак, що, природньо, знизить безпеку зберігання даних. Таким чином, виникає задача зниження часу пошуку і вибірки даних з моніторингу безпеки.

Для вирішення даної задачі пропонується формувати записи подій з моніторингу безпеки у вигляді бази даних, яка дозволить використовувати механізми СУБД для їх обробки. З огляду на те, що дані механізми є спеціалізованими механізмами обробки даних, представлених в форматі записів баз даних, можна припустити, що в даному випадку ми отримаємо зниження часу обробки даних з БД в порівнянні з механізмом прямого пошуку і вибірки даних з масиву векторів записів даних.

Експерементальні дослідження параметрів засобів моніторингу безпеки. Для аналізу ефективності запропонованих засобів моніторингу безпеки з прискореною обробкою даних проведено експериментальні дослідження часу пошуку і вибірки даних з моніторингу безпеки, представлених двояко: у першому випадку – у вигляді файлу як масиву векторів-записів, у другому – у вигляді формату записів бази даних.

У процесі експериментальних досліджень використовувалася локальна комп'ютерна система з наступними характеристиками: процесор Intel Core i7-263QM 2Gz, оперативна пам'ять – 4Гб, яка функціонує під управлінням операційної системи Windows 7. Для аналізу даних з моніторингу безпеки, представлених у вигляді файла-масиву векторів-записів, розроблений спеціальний модуль на мові Java7, а для аналізу даних, представлених в форматі записів бази даних використовувалася СУБД Oracle 10g.

В процесі досліджень оцінювалися такі характеристики: $T_{зб}$ – сумарний час збору даних з моніторингу безпеки (за всіма параметрами вектора X) і запису їх у файл векторів ($T_{зб1}$) або в формат бази даних ($T_{зб2}$); час вибірки даних з моніторингу безпеки $T_{вб1}$, відповідно, засобами Java з файлу векторів-записів ($T_{вб1}$) або вибірки даних в форматі БД з використанням СУБД Oracle ($T_{вб2}$). В результаті оцінювалося сумарний час аналізу даних з моніторингу безпеки $T_{ан}$ розподілених баз даних засобами Java і Oracle як: $T_{ан} = T_{зб} + T_{вб}$.

В процесі експериментальних досліджень генерувалися масиви даних щодо подій моніторингу різної розмірності в діапазоні від 10000 до 100000 (10000, 50000, 100000) векторів-записів, при цьому кожен вектор містив по 10 контрольованих подій.

В таблиці наведено отримані експериментальні дані по записам і обробці подій моніторингу безпеки для засобів на основі Java і Oracle.

Таблиця

Експериментальні дані по записам і обробці подій

№ експе-ри-менту	Розмір-ність, Кз	10000		50000		100000	
	Час Т,с	Java 7	Oracle 10g	Java 7	Oracle 10g	Java 7	Oracle 10g
1	Тзб	0,097	1,265	0,163	8,719	0,208	21,188
	Твб	2,519	0,031	39,948	0,047	163,37	0,109
2	Тзб	0,077	1,211	0,161	8,626	0,238	23,128
	Твб	2,485	0,031	38,348	0,046	156,15	0,062
3	Тзб	0,077	1,362	0,159	8,989	0,284	22,643
	Твб	2,259	0,032	39,562	0,047	144,64	0,081
4	Тзб	0,083	1,269	0,162	8,413	0,245	21,972
	Твб	2,412	0,031	36,216	0,047	158,66	0,083
5	Тзб	0,098	1,271	0,161	8,692	0,272	21,864
	Твб	2,491	0,031	37,143	0,047	152,44	0,101
6	Тзб	0,087	1,311	0,161	8,291	0,291	22,002
	Твб	2,222	0,035	38,921	0,045	161,99	0,103
7	Тзб	0,094	1,27	0,158	8,95	0,283	21,892
	Твб	2,431	0,031	39,443	0,047	159,05	0,098
8	Тзб	0,092	1,376	0,163	8,878	0,256	21,674
	Твб	2,501	0,031	37,248	0,047	163,24	0,101
9	Тзб	0,096	1,324	0,16	8,71	0,209	21,225
	Твб	2,432	0,034	37,549	0,048	149,58	0,087
10	Тзб	0,089	1,291	0,161	8,64	0,243	22,019
	Твб	2,199	0,031	38,243	0,051	152,31	0,108
Середнє значення	Тзб	0,089	1,295	0,1609	8,6908	0,2529	21,960
	Твб	2,3951	0,0318	38,262	0,0472	156,1474	0,0933
Сума	Тан= =Тзб+ +Твб	2,484	1,327	38,423	8,738	156,40	22,054

Всього проведено 10 незалежних експериментів по генерації масивів даних щодо подій моніторингу різної розмірності, далі виконано усереднення отриманих даних. На рис. 3 показана діаграма оцінки сумарного часу аналізу даних щодо подій моніторингу безпеки в розподілених БД засобами Java і Oracle.

Як показали отримані експериментальні дані, з ростом кількості векторів записів за даними моніторингу, істотно зростає виграш за часом аналізу даних з моніторингу безпеки засобами Oracle в порівнянні із засобами Java. При цьому за параметром сумарного часу збору даних з

моніторингу безпеки ($T_{зб1}<T_{зб2}$) засоби на основі Java є більш ефективними, але вони істотно поступаються засобам Oracle по параметру часу вибірки даних з моніторингу безпеки ($T_{вб1}>>T_{вб2}$).

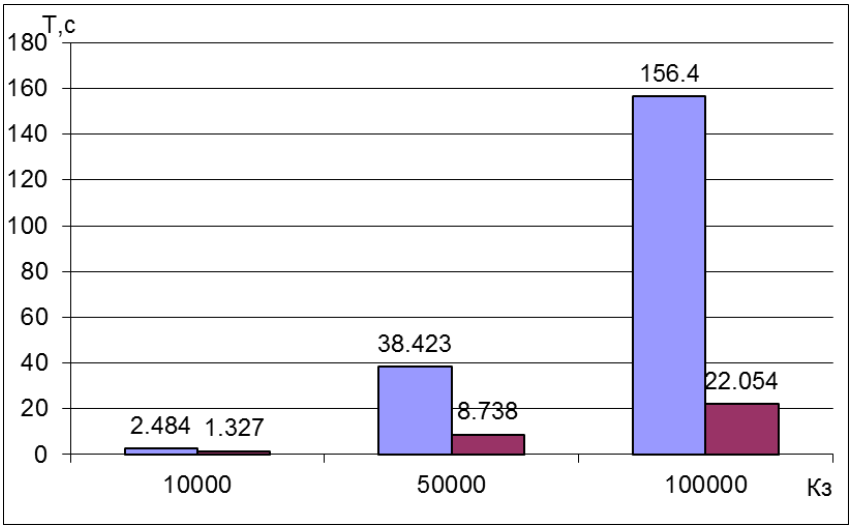

Рис.3. Діаграма оцінки сумарного часу аналізу даних щодо подій моніторингу безпеки

В результаті для 10000 векторів-записів виграш за сумарним часу аналізу даних з моніторингу безпеки ($T_{ан}$) становить 88% (1.88 разів: $T_{ан1}$ =2.48 с для засобів на основі Java і $T_{ан2}$ = 1.32 с для засобів на основі Oracle), а для 100000 векторів-записів – вже понад 800% (7.09 разів: $T_{ан1}$ =156.4 с для засобів на основі Java і $T_{ан2}$ =22.05 с для засобів на основі Oracle). В практичних застосуваннях в системах моніторингу має місце постійне накопичення, тобто зростання числа векторів-записів, таким чином, запропонований підхід дозволяє істотно підвищити швидкість обробки даних з моніторингу безпеки, зокрема, розподілених баз даних.

Висновок. В статті представлена необхідність підтримки реалізації прискореної обробки даних щодо подій моніторингу безпеки для підвищення ефективності аналізу подій безпеки розподілених баз даних. Запропоновано засоби моніторингу безпеки з прискореною обробкою даних. Показано, що, незважаючи на зростаючі обсяги даних щодо подій моніторингу, засоби моніторингу безпеки на основі запропонованого підходу дозволяють динамічно обробляти інформацію з моніторингу безпеки, що забезпечує оперативне формування рівня підозрілості дій

суб'єктів в процесі їх взаємодії з розподіленою базою даних і що дозволить знизити ймовірність вторгнень і атак на базу даних.

Список літератури: 1. *Смирнов С.Н.* Безопасность систем баз данных / *С.Н. Смирнов*. – М.: "Гелиус АРБ", 2007. – 352 с. **2.** *Мельников В.П.* Информационная безопасность и защита информации / *В.П. Мельников*. – М.:"Academiya", 2007. **3.** *Поляков А.* Безопасность Oracle глазами аудитора: нападение и защита / *А. Поляков*. – М.: "ДМК Пресс", 2009. – 336 с. **4.** *Ладыженский Г.М.* Системы управления базами данных / *Г.М. Ладыженский*. – М.: "Jet Infosystems", 2007. **5.** *Гринченко Н.Н.* Проектирование баз данных / *Н.Н. Гринченко, Е.В.Гусев, Н.П. Макаров*. – М.: Горячая Линия-Телеком, 2007. – 468 с. **6.** *Шварц Б.* Базы данных. Оптимизация производительности / *Б. Шварц, П. Зайцев, В. Ткаченко*. – Санкт-Петербург: Символ-Плюс, 2010. – 832 с. **7.** *Герберт Шилдт*. Java 7. Полное руководство / *Шилдт Герберт*. – М.: "Вильямс", 2012. – 1104 с. **8.** *Бородина А.И.* Технологии баз данных и знаний / *А.И. Бородина* – Минск.: БГЭУ, 2008. – 505 с. **9.** *Черноусова А.М.* Создание и использование баз данных / *А.М. Черноусова*. – Оренбург: ГОУ ОГУ, 2009. – 244 с. **10.** *Фуфаев Э.В.* Разработка и эксплуатация удаленных баз данных / *Э.В. Фуфаев, Д.Э. Фуфаев*. – М.:"Academiya", 2010. – 256 с.

Статью представил д.т.н., проф. кафедри ТПТ, проректор НТУУ "КПІ" Варламов Г.Б.

УДК 681.325

Механизмы повышения эффективности процедуры мониторинга безопасности в распределенных базах данных / Мухин В.Е., Корнага Я.И. // Вестник НТУ "ХПИ". Серия: Информатика и моделирование. – Харьков: НТУ "ХПИ". – 2012. – № 38. – С. 128 – 135.

Рассмотрены средства поддержки безопасной обработки данных в распределенных базах данных. Определены основные компоненты системы управлением мониторинга сервера безопасности данных. Предложены средства мониторинга безопасности с ускоренной обработкой данных. Для анализа эффективности этих средств проведены экспериментальные исследования времени поиска и выборки данных по мониторингу безопасности. Ил.: 3. Табл. 1. Библиогр.: 10 назв.

Ключевые слова: базы данных, сервер безопасности, мониторинг, поиск и выборка данных.

UDC 681.325

Mechanisms of increase of efficiency of procedure of monitoring of safety are in the distributed databases / Muhin V.E., Kornaga Ja.I. // Herald of the National Technical University "KhPI". Subject issue: Information Science and Modelling. – Kharkov: NTU "KhPI". – 2012. – №. 38. – P. 128 – 135.

In the paper are considered the mechanisms for secured data processing in distributed databases (DB). The main components of the control system for montoring of the data security server are presented. The security monitoring mechanisms based on the data processing acceleration are suggested. Also, there is performed the experimental analysis of the suggested mechanisms effectiveness on the time of data searching and retrieving. Figs.: 3. Tab.: 1. Refs.: 10 titles.

Keywords: database, server security, monitoring, data search and retrieval.

Надійшла до редакції 26.07.2012