МОДЕРНИЗАЦИЯ ЭКОНОМИЧЕСКИХ СИСТЕМ: ВЗГЛЯД В БУДУЩЕЕ (MESLF-2015)

Сборник научных трудов

Vědecko vydavatelské centrum «Sociosféra-CZ» Praha 2015
«MODERNIZATION OF ECONOMIC SYSTEMS:
LOOKING TO THE FUTURE»
(MESLF-2015)

Collection of scientific papers

Vědecko vydavatelské centrum «Sociosféra-CZ»
Praha 2015

Редакционная коллегия
Kholnazar Amonov - Ph.D, Director for Strategy and Development, CBU
Неверов Павел Александрович – к.э.н., зам зав каф. БУАС по науке, Финансовый университет при Правительстве Российской Федерации.
Аманжолова Бибигуль Ашкеновна – д.э.н., профессор, заведующий кафедрой учета и статистики, Новосибирский государственный технический университет.

Организационный комитет
Petr Hájek, - Ph.D., Vice-rector for Research and International Relations, CBU
Kholnazar Amonov - Ph.D., Director for Strategy and Development, CBU
Alexej Lesnik - Director of International Education, VSEM, CBU

В сборнике научных трудов приводятся основные результаты деятельности ученых, научных коллективов, преподавателей и сотрудников научно-исследовательских и учебных заведений, студентов, магистрантов, аспирантов, по разработке новых элементов и процессов в экономике, юриспруденции, педагогике, технических и сельскохозяйственных наук реализуемых в условиях модернизации экономических систем.

Сборник подготовлен на основе материалов Международной научно-практической конференции «Инновационные процессы в условиях глобализации мировой экономики: проблемы, тенденции, перспективы» (06 ноября 2015 г., г. Прага, Чешская Республика) с участием ученых различных стран.

ISBN 978-80-7526-012-3
DEVELOPMENT OF PROTECTED CARTOGRAPHIC DATABASE
GENERATING PARALLEL MODULE

Gibadullin R., Ph.D.
Rahmatullin F., Master
Riyanov R., student
Kazan National Research Technical University named after A.N.Tupolev
Russian, Kazan
E-mail: landwatersun@gmail.com, rframd@gmail.com, correon39@gmail.com

Annotation: This article explores the possibilities of geographic information system QGIS to work with DBMS PostgreSQL. Software module for parallel encryption/decryption of cartographic data has been developed and its further analyze on test database in order to get experimental evaluation of encryption/decryption speed was made.

Keywords: database management systems, database, geographic information system, encryption, parallel computing, relational database, cartographic database, PostgreSQL.

1. Introduction

Geographic information systems (GIS) are collection, storage, analysis and graphical visualization of spatial data systems and related information on the representation of the object. Data in geographic information systems are stored as a set of thematic layers combined based on their geographic location.

Cartographic data are characterized by high cost of work on its acquisition, in addition, they may contain sensitive information, such as information about the location of new mineral deposits. Therefore, the task of protecting the cartographic data is relevant.

2. Preparation of test environment

The basic functionality of GIS software of major manufacturers almost the same, but enhanced one can vary greatly. A comparison of the most common user-type GIS such as ArcGIS, Mapinfo and QGIS was made. Because of free, open source code, and therefore availability to any user, sufficiently powerful functionality and compatibility with object-relational database management systems, GIS QGIS has been selected for the work.

Databases are particularly popular because of database management systems (DBMS) that implement relational data model. Three major open source database have been considered: SQLite, MySQL, PostgreSQL. PostgreSQL differs from other DBMS because it supports object-oriented and / or relational database approach, also it most closely corresponds to ANSI/ISO SQL standards. Parallelism in PostgreSQL is not achieved by blocking read operations, but through implementation of MultiVersion Concurrency Control (MVCC). It is very easy to expand its procedures, which are called stored procedures. These features simplify the use of constantly repeated operations. That’s why PostgreSQL DBMS has been chosen for this work.

Test database represented by the map of the Russian Federation has been chosen for this work. The data in the open geodata set presented in layers, in vector format. The data is in a geographic coordinate system WGS84, no projection.

3. DBMS setup. Software module development

QGIS and opened in it cartographic Shapefile are installed. DBMS PostgreSQL with PostGIS extension is installed.

First of all it’s necessary to transfer data from QGIS to PostgreSQL. In order to do that Open Database Connectivity driver was used for connecting to PostgreSQL Server. Using database manager tool data from QGIS imported to database.

While working with PostgreSQL there is a need to backup database, restore the database from backup, monitor the status of the server. For this purposes such utilities as pg_dump, pg_restore, pg_ctl were used.
PostgreSQL provides the ability to encrypt data at different levels, which helps to protect data from unauthorized access. Encryption can be used to protect sensitive data such as the location of new deposits, and other financial information. In this paper, and have been used only some of the available encryption mechanisms in the PostgreSQL database.

The project is based on the encryption of certain table columns. Connected pgcrypto module allows to encrypt certain fields and optionally to compress them. In this work fields of geometry type enclosing a location and contours of objects get encrypted, because these fields are the most valuable in the database. The user is given the decryption key with which the data can be decrypted to work on them. Table with encrypted field geom is stored on server in case of decryption, or with a field of type geom that you want to encrypt.

One of the key problems is the choice of encryption algorithm. Three options were considered: aes128, aes192 и aes256. To evaluate the performance of the work with these algorithms were carried out experimental measurements of encryption time of 100,000 cells of the field geom from the table highway-line from test database.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Encryption time (sec.)</th>
<th>Decryption time (sec.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>aes128</td>
<td>170</td>
<td>136,4</td>
</tr>
<tr>
<td>aes192</td>
<td>259</td>
<td>165,4</td>
</tr>
<tr>
<td>aes256</td>
<td>296</td>
<td>194</td>
</tr>
</tbody>
</table>

Algorithm aes128 currently provides a sufficiently strong encryption while showing high performance, that’s why this algorithm has been used in this work.

C# programming language, Windows Forms technology and Visual Studio IDE are used to develop software.

In this software Task Parallel Library (TPL) has been used to organize parallel work. The principle of tasks parallelism is applied. Encryption of column of the table is performed by dividing the main task to several subtasks and their parallel execution.

While developing the software packet processing concept was used.

To test the speed of parallel data encryption / decryption program was launched on the computing cluster node. The first 2000000 cells of the field geom from highway-line table were selected as the test data. 10,000 cells is the amount of the task package.
Table 2 – Measurement results of module’s work time on cluster node

<table>
<thead>
<tr>
<th>Processing speed on cluster node (Intel Xeon E5 2640 2.7GHz, 128Gb ram, mech HDD)</th>
<th>encrypt(sec.)</th>
<th>decrypt(sec.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>12 threads with 10000 cells per packet</td>
<td>454</td>
<td>468</td>
</tr>
<tr>
<td>8 threads with 10000 cells per packet</td>
<td>587</td>
<td>573</td>
</tr>
<tr>
<td>4 threads with 10000 cells per packet</td>
<td>944</td>
<td>907</td>
</tr>
<tr>
<td>2 threads with 10000 cells per packet</td>
<td>1549</td>
<td>1536</td>
</tr>
<tr>
<td>1 thread without packet processing</td>
<td>2336</td>
<td>2265</td>
</tr>
</tbody>
</table>

Usage of parallel technologies increases processing speed up to 5 times in the case of 12 cores against the work on a single core. But during the working process the loading of CPU cores of cluster node is 60% in the case of 12 streams processing. Insufficient speed of the cluster node disk subsystem may be the reason of lower performance growth. In order to check this suggestion, software module was launched on home PC with solid-state drive applying the same testing data.

Table 3 - Measurement results of module’s work time on home PC with solid-state drive

<table>
<thead>
<tr>
<th>Processing speed on home PC (Core i5 3570 4,16GHz, 8 Gb ram DDR3 1384, SSD Plextor m6s)</th>
<th>encrypt(sec.)</th>
<th>decrypt(sec.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 threads with 10000 cells per packet</td>
<td>432</td>
<td>447</td>
</tr>
<tr>
<td>2 threads with 10000 cells per packet</td>
<td>836</td>
<td>746</td>
</tr>
<tr>
<td>1 thread without packet processing</td>
<td>1584</td>
<td>1493</td>
</tr>
</tbody>
</table>

The data obtained by measuring performance using configuration with solid-state drive has shown almost fold increase of performance depending on the number of processor cores that exceed performance cluster node under similar conditions.

**Conclusion**

Acquired experimental data shows that at the current stage of development of processor power so-called "bottleneck" in the parallel processing large amounts of data is likely to be a computer disk subsystem. However, this problem can be solved by using high-speed solid-state drives (SSD) or using server's RAM as a disk drive (ramdisk technology).
МОДЕРНИЗАЦИЯ ЭКОНОМИЧЕСКИХ СИСТЕМ: ВЗГЛЯД В БУДУЩЕЕ (MESLF-2015)

Сборник научных трудов

V autorově vydání
Produkce – I. G. Balašova

Podepsáno v tisku 28.11.2015. 60×84/8 ve formátu.
Psaní bílý papír. Vydavate llistů 29,28, 120 kopii.

Vědecko vydavatelské centrum «Sociosféra-CZ», s.r.o.:
U dálnice 815/6, 155 00, Praha 5 – Stodůlky, Česká republika.
Tel. +420608343967,
web site: http://sociosphera.com,
e-mail: sociosfera@seznam.cz