

Серверная часть системы должна представлять собой два физических сервера: 1) сервер, который непосредственно централизованно управляет светофорными объектами в городе; 2) сервер, обеспечивающий взаимодействие с GPS/GSM устройствами транспортных средств оперативного назначения.

Сервер 1 и сервер 2 физически соединяются между собой. Сервер 1 не имеет доступа к сети интернет, локальным сетям, за исключением сети светофорных объектов. Кроме порта для соединения с сервером 2, все порты на сервере 1 отключены файрволом, в том числе отключена служба ICMP. На сервере 2 также отключены все порты, кроме порта для взаимодействия с терминалами ТС и порта обмена данными с сервером 1.

Внедрение системы приоритетного проезда перекрестков для ТС служб оперативного назначения требует внимательного отношения к компьютерной безопасности. Взаимодействие элементов системы должно происходить по защищенным каналам связи с использованием шифрования и аутентификации. Стабильная, надежная работа серверной части может быть обеспечена при грамотной настройке политик безопасности каждого из серверов.

Работа выполнена при поддержке Европейского гранта «Grant Agreement Number 2013-4550/001-001» по проекту Be-Safe – Белорусская сеть безопасных дорог 544181-TEMPUS-1-2013-1-IT-TEMPUS-JPCR.

Список цитированных источников

1. U.S. DOT (2003). Fatality Analysis Reporting System (FARS) Web-Based Encyclopedia Queries for Emergency Use Crash Statistics.
2. Согоян, А.Л. Система приоритетного движения на перекрестках «Зеленая волна» для транспортных средств оперативного назначения: сб. материалов V Международной научно-технической конференции OSTIS-2015 / А.Л. Согоян, В.Н. Шуть. – Минск: БГУИР, 2015. – С. 309–314.

УДК 004.04

РЕАЛИЗАЦИЯ ОТКАЗОУСТОЙЧИВОСТИ ВЫСОКОНАГРУЖЕННЫХ СИСТЕМ

Шахно М.И.

*Брестский государственный университет имени А.С. Пушкина, г. Брест
Научный руководитель: Козинский А.А., к.пед.н., доцент*

При разработке высоконагруженных веб-систем возникает множество технических проблем. Одной из таких проблем является организация отказоустойчивости системы. Отказоустойчивость решается на различных уровнях. Практическими приемами организации отказоустойчивости является организация кластера серверов (веб-серверов, контейнеров сервлетов), а также репликация (в памяти, базе данных).

Рассмотрим один из приемов организации отказоустойчивости веб-серверов, который предполагает организацию на уровне архитектуры.

При отправке HTTP-запроса (см. [1], [2]) к сервису, его принимает и обрабатывает веб-сервер. Сервер может являться узлом кеширования (не всегда), а так же узлом, где хранится статический контент приложения. HTTP-запрос на выполнение каких-либо логических действий (обработка запросов к базе данных; обработка вычислений и др.) попадает в узел, где происходит балансировка нагрузки.

Узел балансировки нагрузки передает этот запрос на выполнение одному из подузлов. В нашем случае одному из контейнеров сервлетов. Контейнер сервлетов, выполнив требуемую логическую часть, передает результат запросившему сервису. Пример организации описанного подхода представлен на рис. 1.

Представленная архитектура значительно усложняется при наличии сложного масштабируемого вычислительного кластера. Такой кластер служит для обеспечения вычислений сложноструктурированных данных.

Репликация – это прием синхронизации различного рода данных. Например, данных активной сессии между узлами.

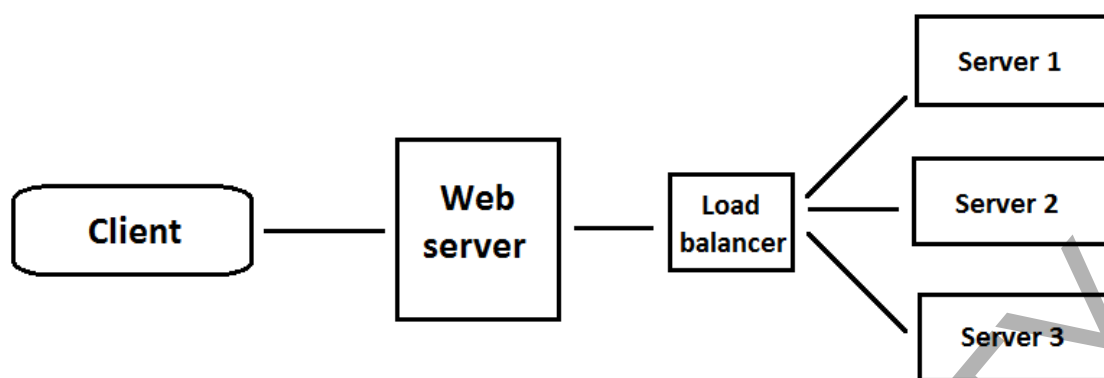


Рисунок 1 – Архитектура отказоустойчивости на уровне серверов

Репликация конфигурируется на подузловых компонентах. В нашем случае такими компонентами являются контейнеры сервлетов.

Данные хранятся в памяти либо выгружаются в базу данных и т.п.

Другим случаем репликации является ее поддержка на уровне баз данных. В случае нескольких баз данных может быть использован подход Master-Slave [3]. В этом случае имеем одну основную базу данных – Master. Изменения в Master фиксируются в бинарном логге, которые затем реплицируются на узел Slave. Такой подход позволяет в случае отказа Master переключиться на Slave. Пример работы представлен на рисунке 2, ниже.

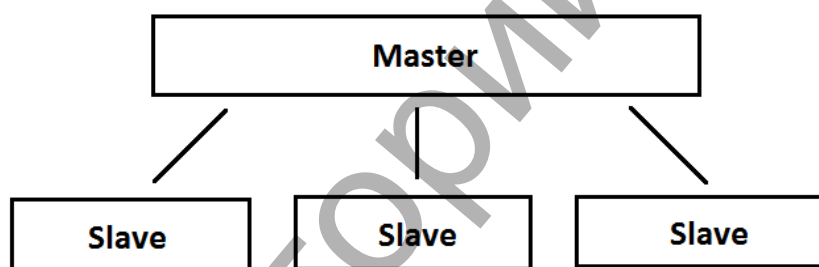


Рисунок 2 – Master-Slave

В ходе доклада будут представлены результаты применения описанных приемов для реализации отказоустойчивости высоконагруженных систем.

Список цитированных источников

1. RFC 2616 [Электронный ресурс] / HTTP/1.1. – Режим доступа: <https://tools.ietf.org/html/rfc2616>. – Дата доступа: 16.10.2015.
2. Простым языком об HTTP [Электронный ресурс] / Простым языком об HTTP. – Режим доступа: <http://habrahabr.ru/post/215117/>. – Дата доступа: 16.10.2015.
3. "What is database replication? – Definition from WhatIs.com" [Electronic resource] / "What is database replication? – Definition from WhatIs.com". – Mode access: <http://searchsqlserver.techtarget.com/definition/database-replication>. – Data access: 15.10.2015.