ФЕДЕРАЦИЯ "НАУКА И ВИСШЕ ОБРАЗОВАНИЕ"
ПРИ ПЛОВДИВСКИ ВИСШИ УЧЕБНИ ЗАВЕДЕНИЯ

СЪЮЗ НА УЧЕНИТЕ В БЪЛГАРИЯ – ПЛОВДИВ

IV НАЦИОНАЛНА

НАУЧНА КОНФЕРЕНЦИЯ 2011

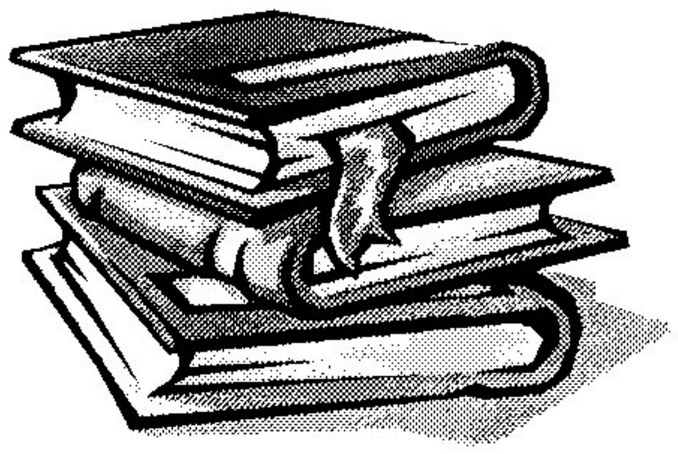
ЗА СТУДЕНТИ, ДОКТОРАНТИ И

МЛАДИ УЧЕНИ

9 години Федерация „Наука и висше образование“
гр. Пловдив

СБОРНИК

/ДОКЛАДИ/



30 април 2011
Пловдив

ISBN: 978-954-9449-44-0

Илеон

Пловдив, 2011

СЕРИЯ 02

ТЕХНИЧЕСКИ И ПРИРОДО-МАТЕМАТИЧЕСКИ НАУКИ

СИСТЕМА ЗА СЪБИРАНЕ, КЛАСИФИЦИРАНЕ, СЪХРАНЯВАНЕ И АНАЛИЗ НА SYSLOG СЪОБЩЕНИЯ

Стоян Попов, Елена Сомова

Резюме: *Статията представя софтуерна система, чиято цел е да разреши основните проблеми, възникващи при работата с логове от множество източници, използващи syslog протокола. Проектиран и реализиран е ефективен метод за класификация на syslog съобщения – дефинират се правила за класификация на съобщенията в дървовидна йерархия от регулярни изрази. Представени са сървърно приложение, което приема, класифицира и изпраща за съхраняване и анализ получените syslog съобщения; уеб-базирано приложение за съхраняване и анализ на логове и RESTful API за комуникация между двете приложения.*

Увод

Всяка компютърна система, независимо от своя хардуер и операционна система, има механизъм за записване на събитията, които се случват с нея (т. нар. логове). Те не представляват интерес за обикновения потребител, но имат ключова роля в работата на системните администратори. Първоначално логовете са използвани само като средство за откриване на проблеми, но в наши дни те служат и за много други цели като оптимизация на системи и мрежи, записване на дейностите, извършвани от потребителите и откриване на неправомерни действия.

Поради масовата употреба на мрежови сървъри, работни станции и всякакви други компютърни устройства и нарастващия брой на възможните проблеми и заплахи, свързани с тях, количеството и разнообразието на генерираните от тези устройства логове значително се увеличава. В организации, използващи стотици компютърни системи, заради ефективното разпределение на ограничен ресурс, с който трябва да се управлява непрекъснато нарастващото количество данни, възниква необходимостта от управление на логовете, което включва създаването, изпращането, съхраняването, защитата и анализа на този тип данни.

В практиката се използват 4 модела за съхраняване на логове в зависимост от броя на системите, които генерират данни и избора на място за съхранение на тези данни: съхраняване във файлове при една система (обикновено на твърдия диск), централизирано съхраняване във файлове при множество системи (обикновено на твърдия диск на сървър), централизирано съхраняване в база данни (на сървър) при множество системи и централизирано съхраняване чрез използване на междинни възли (които събират информация от няколко източника и я предават на един централен сървър). Последният модел е най-широко използван, поради прогресиращото разрастване на системите и мрежите.

Съществуват множество системи, решаващи проблемите, посочени по-горе: syslog-ng [5] за UNIX/Linux с безплатна и платена версия

(syslog-ng Premium Edition), работещи в режими – клиент, междинен възел или сървър; syslog-ng Windows Agent [5] за Windows за режим сървър; Rsyslog [6] с отворен код за UNIX/Linux, BSD и Solaris; WinSyslog [4] за Windows, работещо в режим сървър; Kiwi Syslog Server [2] за Windows с безплатна и платена версия, работещо в режим сървър; уеб базирано безплатно приложение LogAnalyzer [1], използвано с Rsyslog за преглед и анализ на логове; уеб базирано приложение LogZilla [3] за преглед и анализ на съобщения, работещо с syslog-ng и др.

Най-основните недостатъци на съществуващите системи са: работа само с определени операционни системи, ограничени възможности за графичен анализ, липса на възможност за анализ на данните, неудобно и сложно задаване на правилата за филтриране на съобщенията и неефективна класификация на съобщенията.

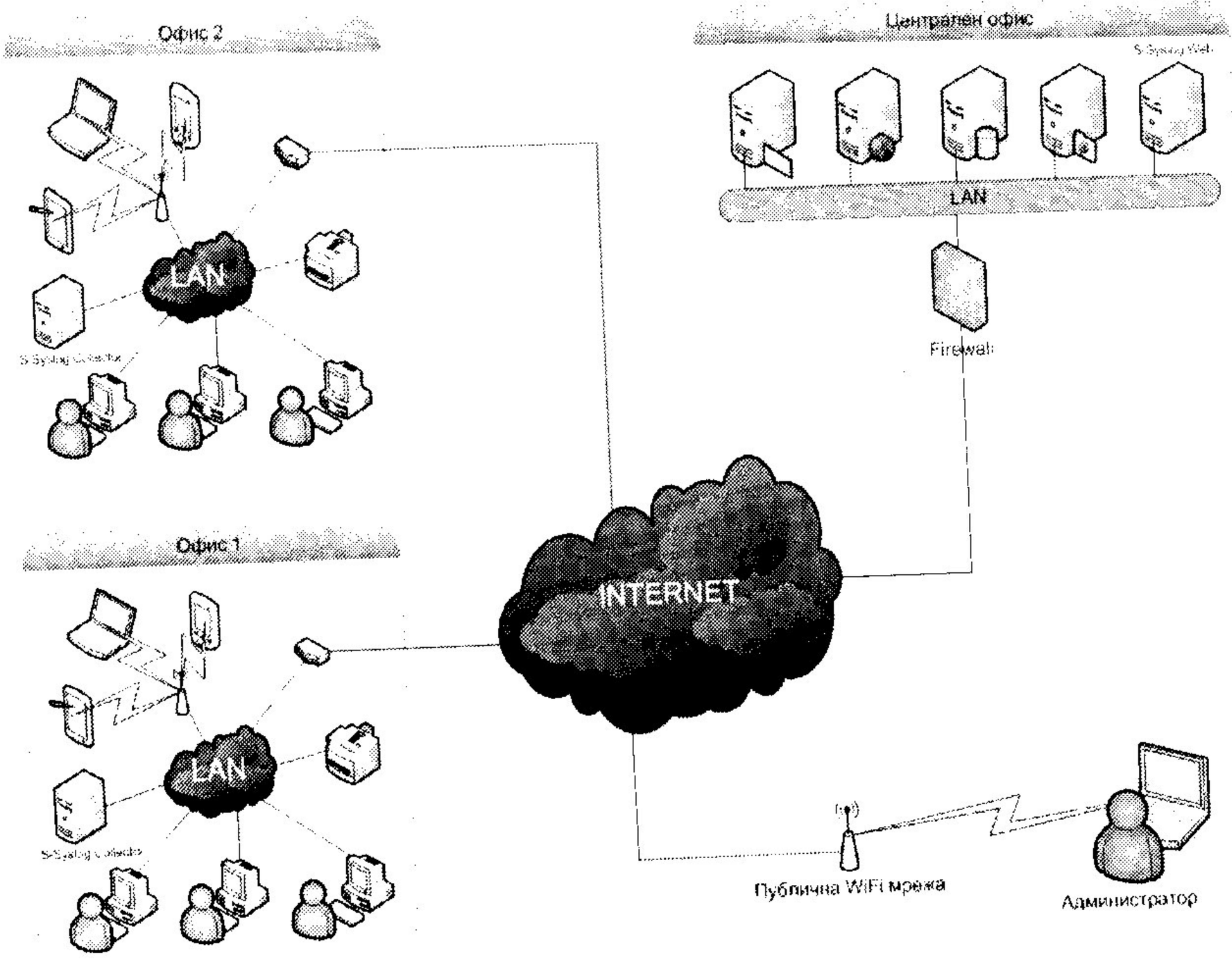
В работата се представя софтуерната система S-Syslog, която прави опит да преодолее основните проблеми, възникващи при работата с логове от множество източници, използващи syslog протокола и да предостави механизъм за ефективна класификация и анализ на данните.

За реализацията на системата се използват следните софтуерни средства: JAVA, PHP, MySQL, JavaScript, YUI, Apache и NetBeans.

Система S-Syslog

S-Syslog е система за събиране, класификация, централизирано съхранение и анализ на събития, регистрирани чрез syslog протокола. Устройствата, които могат да генерират syslog съобщения са персонални компютри, принтери, рутери и други. Системата реализира модела за централизирано съхраняване на логове чрез използване на междинни възли. Тя осигурява едновременно максимална защита на събраната информация и пълен достъп до нея. S-Syslog улеснява процеса на анализ чрез използванео на графики, които могат да се променят от потребителя при необходимост.

Системата (фиг. 1) е съставена от два компонента – S-Syslog Collector и S-Syslog Web. ***S-Syslog Collector*** е JAVA приложение, което работи като syslog сървър и изпълнява ролята на междинен възел. То приема съобщения, класифицира ги и изпраща обработените данни към S-Syslog Web. Там те се съхраняват в база данни, готови за анализ. Комуникацията между двете приложения се изгражда чрез RESTful API.



Фигура 1. Обща схема на работата на S-Syslog

При стартирането си S-Syslog Collector се свързва с S-Syslog Web и използвайки API функции прави заявка за актуалните правила за класификация. След като ги получи се създава тяхно локално копие, което се използва при обработката на данните. При получаването на съобщение то се класифицира и крайният резултат се изпраща към S-Syslog Web. S-Syslog Web дава възможност на системните и мрежовите администратори да следят какво се случва с цялата ИТ инфраструктура на организацията в почти реално време от всяко място и по всяко време.

S-Syslog Collector приема syslog съобщения по 3 различни канала: стандартната за syslog протокола UDP връзка, надеждната TCP връзка и TCP връзка, защитена с SSL. За целта всеки от тях е реализиран като сървърен модул, работещ в отделна нишка, разполагаща със собствени нишки (thread pool). Работа на всяка нишка е да обработи получените данни като крайният резултат е обект, представящ едно syslog съобщение заедно с всичките му характеристики. Създадените обекти, представящи syslog съобщенията, след това се класифицират от други нишки.

За ***класификация на съобщенията*** се използва дървовидна йерархия от регулярни изрази, т. е. правилата за класификация се представят в дърво, чиито възли съдържат регулярни изрази. Нетерминалните възли съдържат регулярен израз, намиращ съвпадение с всеки низ, който може да бъде разпознат от наследниците му. Терминалните възли съдържат регулярни изрази, отговарящи на конкретни правила за

класификация.

Процесът на разпознаване на съобщенията (по самия текст) започва от корена на дървото. При разпознаване на съобщението от някой от неговите наследници, той става текущ възел и процесът продължава. Разпознаването приключва или при достигане до терминален възел или с изчерпването на наследниците на текущия възел. В първия случай съобщението се класифицира точно, а във втория се определя клас от съобщения, към който то принадлежи.

С цел постигане на по-голяма ефективност възлите с общ родител, които са на едно ниво в йерархията, получават различни приоритети. В процеса на класификация първо се обработват възлите с по-висок приоритет. Това дава възможност възлите, разпознаващи най-често срещаните съобщения да бъдат проверявани първи. Задаването на приоритети може да става по два начина – ръчно от потребителя и автоматично.

След натрупване на достатъчно данни приложението може автоматично да определи приоритета на отделните правила въз основа на броя съобщения, които те са класифицирали. Алгоритъмът използва експоненциална плъзгаща се средна стойност на броя успешно класифицирани съобщения от отделните възли с общ родител. Правилата с по-висока средна стойност получават по-висок приоритет. Експоненциална плъзгаща се средна стойност се изчислява по формулата:

$$S_t = \alpha \times Y_t + (1-\alpha) \times S_{t-1}$$

където St е експоненциалната плъзгаща се средна стойност за интервала от време t, Yt е броят на класифицираните съобщения за интервала от време t, α е коефициент, представящ намаляването на влиянието на данните. Чрез коефициента α, при анализа се дава най-голяма тежест на последните (най-близките до текущите) данни.

Накрая класифицираните съобщения се изпращат от отделна нишка към S-Syslog Web посредством извикване на API функция.

Комуникацията между всички участници и S-Syslog Web протича изцяло чрез HTTPS протокола. Това прави невъзможно пасивното подслушване на трафика и осигурява необходимото ниво на сигурност за системата.

S-Syslog Web приложението е изградено в обекто-ориентиран стил на програмиране от няколко модула за: работа със съобщения, графичен анализ, управление на потребителите, системни статистики и работа с правила за класификация. Приложението използва предварително проектиран и реализиран модел за многоезична поддръжка с възможност за лесно добавяне на нови езици.

S-Syslog Web обслужва три групи от потребители, които имат различни права за достъп: API потребители, администратори и анализатори. Правата на ***API потребителите*** са ограничени само до извикването на API функции, които са за четене на правилата за класификация и запис на класифицирани съобщения. ***Анализаторите*** могат да извършват различни действия, свързани с анализа на събраните данни. Те имат достъп до модула за работа със съобщения

и модула за графичен анализ. ***Администраторите*** имат пълен достъп до всички модули на системата.

Модулът за работа със съобщения предлага следните възможности: списък с всички регистрирани събития с възможност за сортиране по показаните характеристики; филтриране на съобщенията по дата, източник, host, тип, класификация и съдържание на съобщението и детайлен преглед на съобщение.

Модулът за графичен анализ предлага следните дейности: задаване на филтри за съобщенията, участващи в анализа – дата, източник, host, тип, класификация и съдържание на съобщението; графики на съобщенията, групирани по час, ден от седмицата, седмица, месец или година и графики на съобщенията, групирани по зададен критерий – тип, източник, класификация.

Модулът за управление на потребителите предлага следните функционалности: списък с всички потребители; добавяне на нов потребител; изтриване на потребител; редактиране на данните на потребител и блокиране на достъпа на потребител.

Модулът за системни статистики предлага следните възможности: списък с IP адрес, дата и час на последното влизане на всеки от потребителите на уеб интерфейса; списък с IP адрес, дата и час на последното влизане на всеки от API потребителите; брой регистрирани съобщения за последните 24 часа и използвано дисково пространство от базата данни.

Модулът за работа с правила за класификация има следните дейности: дървовидно представяне на наличните правила; добавяне на ново правило; редактиране на съществуващо правило; изтриване на съществуващо правило; преместване в дървото на съществуващо правило и автоматично определяне на приоритетите на правилата на дадено ниво въз основа на натрупаните до момента данни.

Заключение

Изградената чрез RESTful API комуникация между двете приложения прави лесно разработването на допълнителни приложения, които да използват функционалностите, предлагани от S-Syslog Collector и S-Syslog Web и да разширят възможностите на системата.

Разработката е частично финансирана по проект ДО 02-308 към Националния научен фонд.

Литература

[1] Adiscon LogAnalyzer – syslog web viewer, analysis and reporting tool, http://loganalyzer.adiscon.com/

[2] Kiwi Syslog, http://www.kiwisyslog.com/kiwi-syslog-server-overview/

[3] Logzilla is Syslog | Proactive Network Management Using Syslog - LogZilla, http://www.logzilla.pro/

[4] Syslog for Windows – The Enhanced Syslog Daemon for the Windows Platform, http://www.winsyslog.com/

[5] syslog-ng – Multiplatform Syslog Server and Logging Daemon,

http://www.balabit.com/network-security/syslog-ng
[6] The enhanced syslogd for Linux and Unix rsyslog, http://www.rsyslog.com/

Стоян Христов Попов, доц. д-р Елена Петрова Сомова
ПУ „Паисий Хилендарски", тел.: 032-261-259
stoyan.popov@gmail.com; eledel@uni-plovdiv.bg

SPECIAL FINITE DIFFERENCE SCHEME FOR THE BLACK-SCHOLES PDE

Mariyan Milev, Milena Petkova

Резюме. *В настоящата статия изследваме проблемът за оценяване на опции, използвайки модела на Black-Scholes, описващ случайното движение на цените на финансовите активи. Основният принос е прилагането на нов вариант на стандартната явна схема на крайни разлики за оценяване на опции, която преди е считана за неефективна, тъй като изисква малка стъпка по времето.*

Ние трансформираме частното диференциално уравнение на Black-Scholes в уравнение на топлопроводност с постоянни коефициенти. Използваме super-time-stepping процедура по времето, която ускорява значително явната схема, освобождавайки я е от ограничението за стабилност на стъпката по времето.

Abstract. *In the present paper we explore the problem for pricing options utilizing the Black-Scholes model for the random movement of the asset price. Our main contribution is that we manage to apply a new variant of the standard explicit finite difference scheme for pricing options that was previously considered inefficient as it requires a prohibitively small time-step. We transform the Black-Scholes partial differential equation to a heat equation with constant coefficients. We use a super-time-stepping as an acceleration procedure which impressively speeds up the explicit scheme by liberating it from the stability restriction on the time-step.*

Keywords: Explicit Finite Difference Schemes, Super-time-stepping, Stability Restriction, Acceleration Methods, Black-Scholes Model, Discrete Barrier Options, Exotics

1. Introduction

In this paper we propose a *new super-time-stepping explicit finite difference method* (STS) for pricing options without closed-form valuation formulas such as discrete double barrier knock-out options. In Section 2 we present a mathematical model for the random movement of the asset price. The option price is specified as a *solution of the parabolic Black-Scholes partial*