Модерирует : lynx, Crash_Master, dg, emx, ShriEkeR

UncoNNecteD

Silver Member

Редактировать | Профиль | Сообщение | ICQ | Цитировать | Сообщить модератору

Есть лог такого вида -
1034456544.292 295 21.31.125.0 TCP_CLIENT_REFRESH_MISS/200 535 GET http://www.....

Вопрос в том что это значит и как расшифровать время и объем отсюда...

Код:

```
http://www.squid-cache.org/Scripts/ - коллекция скриптов для анализа логов squid
http://squid.org.ua/Scripts/ - тот же документ на русском
http://www.opennet.ru/prog/mid/26.shtml#100 - коллекция анализаторов логов squid
```

Анализаторы логов для Squid

Free-SA
Сайт проекта: http://free-sa.sourceforge.net/
Быстрый и легкий в использовании анализатор логов для squid и не только!

SquidLog
Сайт разработчика: http://shleps.narod.ru/soft/squidlog/ (Шлепсик - мой хороший друг)
freeware

sarg
Офф. сайт: http://inter.rags.ru/orso/ (http://unixdocs.rags.ru/sqmgrlog.html)

Цитата:

Генератор отчетов на основании анализа лог-файла прокси сервера Squid. Отчеты позволяют выяснить какой пользователь в какое время обращался к какому сайту.Суммарный отчет может оказать большую помощь в тарификации работающих через Squid пользователей, так как включает в себя суммарный трафик и число коннектов для каждого пользователя за определенный период времени.

Statman
Офф. сайт: http://cyberos.narod.ru/statman/

Цитата:

GPL система мониторинга и управления пользователями SQUID. Реализовано: позволяет задавать лимиты пользователям из разных груп SQUID, тарифы, автоматическое отключение при превышении лимита, отчеты, практически он-лайн просмотр статистики пользователей.

squidGuard
Офф. сайт: http://www.squidguard.org/

Цитата:

быстрая и гибкая система для фильтрации контента и управления доступом для прокси сервера Squid (запускается как внешняя программа редиректа). Ограничение доступа к определенным web-страницам и web-серверам, разграничение доступа для пользователей и групп, поддержка регулярных выражений, блокировка попыток доступа к заблокированному ресурсу по IP адресу, богатые возможности редиректа при ошибке доступа (например, на страницу с правилами или для регистрации), дополнительные ограничения по времени суток и т.д.

Calamaris
Офф. сайт: http://cord.de/tools/squid/calamaris/

Цитата:

parses logfiles from Squid, NetCache, Inktomi Traffic Server, Oops! proxy server, Novell Internet Caching System, Compaq Tasksmart or Netscape/iplanet Web Proxy Server and generates a report. Written in perl5.

Sawmill

Цитата:

http://www.sawmill.net - это вообще какой-то супер-навороченный анализатор всяческих логов, с графиками и хранением всех результатов анализа в базе данных. Среди всего прочего, может и squid анализировать. Можно скачать и посмотреть, что за софт. На сайте есть картинки, примеры, и т.д.

SAMS - SQUID Account Management system
http://sams.perm.ru

Цитата:

Программа для настройки и администрирования доступа пользователей к прокси-серверу SQUID с использованием авторизации ntlm в домене Windows.

SAcc - Squid Accounting
http://sacc.cybersec.ru
Описание на русском: http://sacc.security.perm.ru/about.php

Цитата:

основные возможности:
+максимально оптимизированный принцип работы с данными, в режиме кратких логов -
экономия дискового пространства, при траффике в 6 гб, и количестве пользователей
~105, объём базы данных ~980 Kb
+аутентификация в принципе любая (я использую аутентификацию в Active Directory windows 2000 domain на одной системе и ncsa на другой.)
+отключает по факту превышения в течении 1 секунды или после обработки 20 записей (настраивается).
+устойчива к ошибкам в логе, (пропускает записи для неизвестных пользователей,
но пишет в системный журнал факт такой записи) и падениям сервера или БД.
+разработано с учётом возможных падений, и принципиально не может пропустить ниодной строчки лога.
+возможно полное хранение логов в базе, детализированный режим. С получением информации по каждому запросу для выбранного пользователя.

+В облегчённом режиме логи не хранятся в базе, хранится лишь информация по сайтам,
и информация по пользователям. За счёт этого получаются быстрые выборки и минимальные системные требования. (рекомендуется для слабых систем). В полном режиме хранится вся информация.
+автоматически следит за размером лога, и если лог оказался меньше чем был - начинает
пересчитывать с начала лога (т.е. произошла внешняя архивация логов)
+Вебинтерфейс на PHP и использует MySQL. Демон написан на c++ для максимальной скорости.

Lightsquid
Домашняя страница
+ fast log parser generate small per user data file
+ perl based cgi script for dynamic generated report pages
+ html template for design
+ no database required
+ no additional perl module
+ varios reports
+ user group suport
+ graphics report (v 1.6+)
multilangual interface (English,Russian,Italian,Hungarian,Portuguese – Brazil,Bulgarian,Spanish,Czech)
Для нескольких сотен человек - вещь, как мне кажется, незаменимая. Для тысяч может и медленновата, но для не очень большого кол-ва пользователей - супер. Графики позволяют визуально быстро оценить положение дел.

Всего записей: **4033** | Зарегистр. **21-03-2002** | Отправлено: **09:45 14-10-2002** | Исправлено: **Alukardd**, **20:46 30-01-2011**

Dmitry68

Advanced Member

Редактировать | Профиль | Сообщение | Цитировать | Сообщить модератору

Точно не скажу, но есть программка sarg, которая все это делает:
http://web.onda.com.br/orso/sarg.html

Всего записей: **660** | Зарегистр. **08-04-2002** | Отправлено: **09:59 14-10-2002**

UncoNNecteD

Silver Member

Редактировать | Профиль | Сообщение | ICQ | Цитировать | Сообщить модератору

Просто - у меня есть данные о трафике в определенный момент - мне надо узнать что конкретно кто и что качал через прозрачный прокси.

• Мой-борд

Всего записей: **4033** | Зарегистр. **21-03-2002** | Отправлено: **11:27 14-10-2002**

ooptimum

Silver Member

Редактировать | Профиль | Сообщение | ICQ | Цитировать | Сообщить модератору

UncoNNecteD
Та же беда... SARG -- это да, но иногда надо что-то особенное. Я ничего не нашел. Вот уже несколько дней как собираюсь сам что-нть написать. С трогать не буду сейчас, а вот Kylix для этого -- самое ага.

Всего записей: **2718** | Зарегистр. **30-05-2002** | Отправлено: **14:04 14-10-2002**

UncoNNecteD

Silver Member

Редактировать | Профиль | Сообщение | ICQ | Цитировать | Сообщить модератору

sarg -convert >/file
мне помог
Только вот видно из-за прозрачного проксирования в ip везде стоит адрес типа 21.31.125.0 - то есть как адрес подсети... а вот как вытащить реальный ip'шник качающего я не знаю

• Дизайн и программирование веб. Рубордовцам скидко!
• Мой-борд

Всего записей: **4033** | Зарегистр. **21-03-2002** | Отправлено: **15:24 14-10-2002** | Исправлено: **UncoNNecteD**, **15:25 14-10-2002**

greys

Full Member

Редактировать | Профиль | Сообщение | ICQ | Цитировать | Сообщить модератору

UncoNNecteD
твоя строчка

1034456544.292 295 21.31.125.0 TCP_CLIENT_REFRESH_MISS/200 535 GET http://www.....
расшифровывается так:

когда_был_запрос сколько_длился_запрос удаленный_хост код_запроса/статут_запроса размер_запроса метод_HTTP URL_запроса

А поля эти значат такие вещи:

1. Время, когда был обслужен запрос. Это стандартное Epoch time. Чтобы перевести в понятные циферки, делай что-нибудь такое (это на Перле):
$time=1034456544.292;
($sec,$min,$hour,$mday,$mon,$year,$wday,$yday,$isdst)=localtime($time);

2. Время обслуживания запроса - т.е. сколько милисекунд твой Squid получал страничку и отдавал ее клиенту

3. IP удаленного хоста, откуда читался запрос

4. Код выполнения запроса. По нему можно увидеть, был ли запрошенный объект уже в кеше, или его пришлось получать заново. Или он был, но его пришлось обновить.
В твоем случае, объекта в кеше был, но когда Squid спроил по URL'у, менялся ли запрашиваемый объект, ему ответили, что менялся, и прислали новую версию.

5. Статус выполнения запроса. число 200 это успешное завершение, 403 это редирект, 500 это ошибка сервера. Кодов куча, в сети можно найти описание. Но 200 в твоем случае означает, что все прошло нормально.

6. Количество байт в транзакции, сколько занимал скачанный и переданный клиенту запрос.

7. Метод HTTP запроса для скачивания объекта. Это GET, POST, HEAD.

8. Собственно URL того что запрашивал клиент

На самом деле, там дальше еще несколько полей могут быть, если кэш обращался к своим соседям (peer'ам), но раз ты не написал их тут, то и я объяснять их пока не буду.

Вот такие вот объяснения, надеюсь, понятно объяснил.

А еще, господа, гляньте на следующие ссылки:

www.sawmill.net - это вообще какой-то супер-навороченный анализатор всяческих логов, с графиками и хранением всех результатов анализа в базе данных. Среди всего прочего, может и squid анализировать. Можно скачать и посмотреть, что за софт. На сайте есть картинки, примеры, и т.д.

А вот тут есть тонна сылок на различные скрипты-анализаторы squid'овских логов, уж что-нибудь полезное точно найдется:

http://www.squid-cache.org/Scripts

Ну, всем удачи,
greys

Всего записей: **589** | Зарегистр. **18-10-2001** | Отправлено: **15:31 14-10-2002**

UncoNNecteD

Редактировать | Профиль | Сообщение | ICQ | Цитировать | Сообщить модератору

Silver Member

greys
Спасибо за то что все разжевал, но эти проблемы я уже порешал при помощи sarg.
У меня проблемма только с удаленным хостом - всегда пишет xx.xx.xx.0
Как узнать реальный ip того кто качал конкретный ресурс?

- Дизайн и программирование веб. Рубордовцам скидко!
- Мой-борд

Всего записей: **4033** | Зарегистр. **21-03-2002** | Отправлено: **23:29 14-10-2002**

korvin

Редактировать | Профиль | Сообщение | Цитировать | Сообщить модератору

Junior Member

UncoNNecteD
В squid.conf есть параметр client_netmask, так вот похоже он у тебя стоит 255.255.255.0, если так поставь 255.255.255.255. Должно сработать.

Всего записей: **35** | Зарегистр. **31-05-2002** | Отправлено: **08:40 15-10-2002**

UncoNNecteD

Редактировать | Профиль | Сообщение | ICQ | Цитировать | Сообщить модератору

Silver Member

korvin
Верно подмечено... жаль раньше я этого не знал... и даже не замечал... теперь фиг восстановишь то что было 

Спасибо - исправил на 255  Нефиг маскироваться!

- Дизайн и программирование веб. Рубордовцам скидко!
- Мой-борд

Всего записей: **4033** | Зарегистр. **21-03-2002** | Отправлено: **10:27 15-10-2002**

zenia

Редактировать | Профиль | Сообщение | Цитировать | Сообщить модератору

Я использую sarg.

Junior Member

Как его нужно запустить, с каким ключом или какие настройки нужно сделать в конфиге, чтобы он в Topuser Report суммировал по каждому ip, а то он сейчас выдает по каждоиу подключению.

Всего записей: **151** | Зарегистр. **17-01-2003** | Отправлено: **13:43 15-09-2003**

EndoR

Редактировать | Профиль | Сообщение | ICQ | Цитировать | Сообщить модератору

Advanced Member

Возникла проблема - отключать юзерей при превышении лимита. В данный момент тоже юзаю sarg для отчетов, и в нем натолкнулся на тег per_user_limit. Никаких внятных описаний я не нашел. Что это такое и как это можно использовать?

Fear is an efficient tool of management.

Всего записей: **1159** | Зарегистр. **24-01-2002** | Отправлено: **21:35 24-10-2003**

---

johnikus

Редактировать | Профиль | Сообщение | Цитировать | Сообщить модератору

Newbie

per_user_limit file mb
сохраняет юзеров переваливших порог в указанный файл
а отключать их можно в самом сквайде брать имена из этого файла
например
acl kachki acltype "file"
где acltype тип который используется для авторизации пользователей
а file файл созданный sarg
и далее http_access deny kachki
и заставлять squid перечитывать содержимое файла переодически

Всего записей: **4** | Зарегистр. **11-03-2003** | Отправлено: **04:21 27-10-2003**

EndoR

Редактировать | Профиль | Сообщение | ICQ | Цитировать | Сообщить модератору

Advanced Member

У меня логи сквида каждый день ротейтятся. А через 20 мин запускает сарг и парсит их. Но проблема в том, что нельяз посмотреть статистику за период (например, за месяц). Оригинальные логи сквида ессно через 10 дней перезаписались, и осталась только статистика, сгенеренная саргом. Как можно воссоздать статистику за интервал? Пока на ум пришел только самый плохой вариант - писать скрипт, чтоб он из логов выдирал числа и создавал новую статистику. Кто что может посоветовать?

Fear is an efficient tool of management.

Всего записей: **1159** | Зарегистр. **24-01-2002** | Отправлено: **02:12 21-11-2003**

Domed

Редактировать | Профиль | Сообщение | Цитировать | Сообщить модератору

Newbie

Всем привет!!
Подскажите можно ли при помощи Squid-а запретить доступ определенному пользователю при условии если он исчерпал свой лимит использования Internet (например 20Mb), если можно то как.

Заранее благодарен.

Всего записей: **5** | Зарегистр. **21-11-2003** | Отправлено: **10:08 24-11-2003**

---

lynx

Редактировать | Профиль | Сообщение | Цитировать | Сообщить модератору

Advanced lynx

Domed

При чем тут анализаторы логов то:
Вот твоя тема:

SQUID: ограничить трафик для отдельного юзера [?]

И вообще:
http://forum.ru-board.com/forums.cgi?action=filter&forum=8&filterby=topictitle&word=Squid

Всего записей: **11712** | Зарегистр. **08-05-2001** | Отправлено: **21:47 24-11-2003** | Исправлено: **lynx**, **21:48 24-11-2003**

BeerLion

Advanced Member

Редактировать | Профиль | Сообщение | Цитировать | Сообщить модератору

Есть сеть с виндовыми рабочими местами и RedHat-прокся со squid.
Подскажите плиз, какие скрипты подходят для того, чтобы каждый юзер мог лично

смотреть свою статистику (daily, monthly и т.д и т.п) через браузер.
Для админских целей-то всё что я видел подходит, тут вариантов выбора больше.
Раньше прокся была под виндой с вингейтом, под него я своё ПО писал, теперь пока нет времени под линухами особо ковыряться.
Что больше подходит?

Всего записей: **1330** | Зарегистр. **22-10-2002** | Отправлено: **18:28 26-11-2003**

BeerLion

Advanced Member

Редактировать | Профиль | Сообщение | Цитировать | Сообщить модератору

Всем спасибо
Всё сам написал на перле, который видел последний раз два года назад.

Ну, может же быть такое, что никто не знает, чего обижаться. А вот скрипт свой мог бы и выложить для народа. lynx.

Всего записей: **1330** | Зарегистр. **22-10-2002** | Отправлено: **19:38 06-12-2003** | Исправлено: **lynx**, **03:18 07-12-2003**

EndoR

Advanced Member

Редактировать | Профиль | Сообщение | ICQ | Цитировать | Сообщить модератору

Сейчас вот увидел, что горячо любимый мною SARG уже не поддерживается (23-04-2003 о многом говорит). К тому же начал в даун выпадать иногда. Естественно поднялся вопрос - какая может быть замена? кто что юзает? вебалайзер не подходит.
Основные требования - список пользователей (идеально, если можно в группы объединить ака подразделения, чтобы самому потом с калькулятором не сидеть), кто куда во сколько ходил и сколько налазил с сортировкой по различным категориям (объем, число хитов, время и т.п.).

Fear is an efficient tool of management.

Всего записей: **1159** | Зарегистр. **24-01-2002** | Отправлено: **16:58 22-06-2004**

maxiva

Junior Member

Редактировать | Профиль | Сообщение | Цитировать | Сообщить модератору

EndoR

Два момента:
1. Версия: Last change: Apr/25/2003 sarg-1.4.1.tar.gz
2. Ссылка в шапке не верная. Правильно так: http://sarg.sourceforge.net/sarg.php

SARG ChangeLog
Apr/25/2003: - fixed: - link error to denied site in squidGuard report
- resolve name error in squidGuard report
- some fixes to HPUX. Thanks to Miles Roper <mroper@westcoastdhb.org.nz>
- index_sort_order tag don't work correctly.
- too many open files fixed. Thanks to Francesco Perrillo <fperillo@totalfax.it>

- Ukrainian_windows1251 included in sarg.conf file
- exclude_string don't work correctly.

Плюс к этому (цитирую):
Patches:
How to apply: save the patch in sarg-1.4.1 directory, patch -p0 < _patch_name, make install
sarg-1.4.1-index.sort.patch - index sort fixed.
http://sarg.sourceforge.net/sarg-1.4.1-index.sort.patch.gz

Цитата:
> К тому же начал в даун выпадать иногда. Естественно поднялся вопрос - какая может быть замена?

По пунктам: последняя версия - абсолютно стабильная. Поэтому следующая и не вышла. Глюков не отмечено. Если Вы качали не с оф. сайта и собирали ее не с теми библиотеками (кстати, а ваша система и gcc - ?), то неизвестно, что вообще у вас стоит.

Юзаю уже давно, работает изумительно, все по-русски (для начальства), никаких проблем не замечал.

Всего записей: **100** | Зарегистр. **24-09-2002** | Отправлено: **10:22 25-06-2004** | Исправлено: **maxiva**, **10:41 25-06-2004**

EndoR

Редактировать | Профиль | Сообщение | ICQ | Цитировать | Сообщить модератору

Advanced Member

maxiva
на офф сайте впащет ссылка стоит на сорсфордж.

Цитата:
> то неизвестно, что вообще у вас стоит

и версия сарга у меня тоже с оффсайта. и системы разные - redhat 9.0 и freebsd 5.2.1.

Цитата:
> Глюков не отмечено

Цитата:
> Юзаю уже давно, работает изумительно, все по-русски (для начальства), никаких проблем не замечал

и у меня работает уже больше 2,5 лет, и бывают глюки. иначе не писал бы я сюда.

Fear is an efficient tool of management.

Всего записей: **1159** | Зарегистр. **24-01-2002** | Отправлено: **14:05 05-07-2004**

НОВАЯ ТЕМА | СОЗДАТЬ ОПРОС | ОТВЕТИТЬ

Страницы: **1** 2

Имя:

Пароль:

Сообщение

Для вставки имени, кликните на нем.

Загрузить виртуальную клавиатуру

Автозакрытие тэгов

Опции сообщения

- Добавить свою подпись
- Подписаться на получение ответов по e-mail
- Добавить тему в личные закладки
- Разрешить смайлики?
- Запретить коды

Отправить

Переход по форумам