ISBN 5-94052-066-0 ПРОГРАММНЫЕ СИСТЕМЫ: ТЕОРИЯ И ПРИЛОЖЕНИЯ. ПЕРЕСЛАВЛЬ-ЗАЛЕССКИЙ, 2004

УДК 681.324

В. В. Парменова

Адаптация мониторной системы MON для системы коммуникаций «Ботик»

Аннотация. Система телекоммуникаций «Ботик» использует мониторную систему MON для наблюдения за состоянием городской компьютерной сети. Система MON является свободно-распространяемым программным обеспечением. Именно поэтому имеется возможность изменять и дополнять ее. В работе рассказывается о модификациях, внесенных в мониторную систему MON, с целью удовлетворить дополнительным требованиям, а именно: улучшение системы оповещения, создание нового Web-интерфейса, повышение качества проверок. Описывается функциональность и принципы работы системы. Особое внимание уделяется дополнениям и модификациям системы MON.

Ключевые слова и фразы: Региональные сети, мониторная система, система мониторинга, работоспособность сетевого оборудования.

1. Введение

1.1. Постановка задачи. Система мониторинга технического состояния сети MON используется СТ «Ботик» для наблюдения за состоянием городской компьютерной сети[1]. Мониторинг сети системой MON осуществлялся достаточно продолжительный промежуток времени, что позволило оценить работу мониторной системы и заметить некоторые ее недостатки, а именно:

(1) недостаточная тщательность проверки оборудования либо сервиса, что приводило к ложным срабатываниям системы оповещения, либо пропуск серьезных поломок в сети;
(2) избыточность сообщений об одной и той же поломке — это приводит к ослаблению бдительности обслуживающего персонала сети, особенно если поломка незначительная и легко устранимая;

Работа выполнялась при частичной поддержке Суперкомпьютерной Программы «СКИФ» Союзного Государства и программы фундаментальных научных исследований ОИТВС РАН «Новые физические и структурные решения в инфотелекоммуникациях».

[1]В данной работе под словами “городская компьютерная сеть” понимается система телекоммуникаций (СТ) «Ботик» города Переславля-Залесского.

(3) неудобный формат письма о проблеме в сети — необходимо просмотреть большое количество второстепенной информации, прежде чем будут предоставлены основные данные о результатах проверки;
(4) неинформативный Web-интерфейс, содержащий очень мало детальной информации о ситуации в сети.

Кроме того, систему MON невозможно использовать для проверки целостности каналов связи. При наличии в сети резервных линий ping-тест, который используется для проверки работоспособности маршрутизаторов, не дает достоверной информации о строении и неизменности графа коннективности.

Таким образом, были сформулированы требования к мониторной системе, которые позволили бы сделать процесс наблюдения за работой сети более качественным и удобным. Так как система MON является свободно-распространяемым продуктом, есть возможность внести в нее свои модификации и удовлетворить этим требованиям. К указанным требованиям прежде всего относятся:

(1) повышение качества проверок — мониторная система должна уметь отличать серьезную поломку от незначительного сбоя в работе сети с последующим самовосстановлением;
(2) оповещение о поломке в сети, а также оповещение о восстановлении работоспособности оборудования (сервиса), даже если восстановились не все компьютеры в группе, а только часть из них;
(3) представление результатов проверок в Web по всем параметрам проверки и в любой момент времени;
(4) создание дополнительных мониторных программ, которые могут быть использованы системой MON, для наблюдения за неизменностью графа коннективности для проверки сети на наличие разрывов на линиях.

Модифицированная версия системы MON должна удовлетворять всем вышеперечисленным требованиям. Целью настоящей работы была разработка такой модификации системы MON, которая осуществляет более тщательную проверку сервисов, сообщает персоналу более точную информацию о ситуации в сети и отображает результаты проверок в Web.

2. Архитектура системы MON

2.1. Компоненты и функциональность. Система MON состоит из следующих компонент:

(1) конфигурационные файлы системы MON;
(2) daemon (демон) — основная часть системы, координирующая действия всех остальных ее частей;
(3) набор мониторов — программ, производящих проверку сервисов и оборудования, каждый монитор может производить проверку только одного сервиса;
(4) набор программ, осуществляющий оповещение;
(5) журнал системы.

Перед началом эксплуатации системы необходимо сформировать для нее конфигурационные файлы. В них указываются параметры проверок, а именно:

(1) группы компьютеров (маршрутизаторов, серверов), которые должны подвергаться проверке;
(2) сервисы, которые должны проверяться на указанных группах компьютеров и, если необходимо, специальные параметры проверок;
(3) время проведения проверок и интервалы между проверками;
(4) методы оповещения, частота посылки сообщений, адреса.

Пример конфигурационного файла показан на рисунке 1.

После того, как конфигурационные файлы будут написаны, можно запускать систему. Основной процесс (daemon, демон) после запуска будет работать до тех пор, пока не будет остановлен специальной linux-командой. С интервалом, определенным в конфигурационном файле, основной процесс запускает программы-мониторы для проверки работоспособности сети. Вся информация о мониторах и проверяемых компьютерах читается один раз из конфигурационного файла и впоследствии используется демоном для запуска соответствующих мониторов.

После того, как монитор выполнил свою проверку, он возвращает основному процессу некоторое число, соответствующее результатам работы монитора. Например, если проверка показала, что все проверяемые машины работоспособны, монитор возвращает 0, в противном

```
# Пути к основным рабочим директориям

cfbasedir    = /etc/mon
alertdir     = /usr/lib/mon/alert.d
mondir       = /usr/lib/mon/mon.d

# Группы компьютеров, которые необходимо проверять.

hostgroup FirstGroup host1.domain1.com host2.domain1.com

hostgroup SecGroup server1.domain2.com server2.domain2.com

# Параметры проверок

watch FirstGroup
    service fping
    description ping-test
    interval 10m
    monitor fping.monitor
    period wd {1-4} hr {8-20}
         numalerts 2
     alert mail.alert root@host1.domain1.com
     upalert mail.alert root@host1.domain1.com

watch SecondGroup
    service http
    description http port check
    interval 1h
    monitor http.monitor
    period wd {2-6} hr {4-23}
         numalerts 5
     alert mail.alert root@host1.domain2.com
```

Рис. 1. Пример конфигурационного файла системы MON

случае возвращаемое значение будет равно 1. Кроме числового значения основной процесс получает от монитора информацию о ходе и результах проверки, представленную в текстовом виде. Такая информация передается основному процессу в случае если где-то найдена неполадка.

Далее основной процесс решает, нужно ли послать сообщение о поломке или оно уже было отправлено. Демон следит за количеством

сообщений — оно не должно превышать указанное в конфигурационном файле. Если сообщение должно быть послано, демон вызывает соответствующую программу оповещения, передает ей информацию о получателе и текст с описанием проблемы, полученный от монитора. Программа оповещения принимает переданные ей аргументы и рассылает сообщения.

Демон может также вызвать программу оповещения, если необходимо сообщить персоналу о восстановлении ранее неработоспособного сервиса. Это делается только в том случае, если соответствующая строка (`UPALERT`) присутствует в конфигурационном файле. Сообщение о восстановлении будет отправлено только если все компьютеры в группе работоспособны (то есть демон получил значение 0 от монитора).

По истечении интервала времени, указанного в конфигурационном файле, основной процесс снова запускает монитор и процесс повторяется.

В системе MON имеется более сорока мониторных программ. Из них наиболее востребованными (в случае СТ «Ботик») являются: fping.monitor, проверяющий доступность компьютеров по протоколу ICMP, ftp.monitor, http.monitor, smtp.monitor, pop3.monitor, imap.monitor, и некоторые другие, проверяющие работоспособность соответствующих сервисов. С помощью монитора freespace.monitor MON предоставляет возможность отслеживать количество свободного места на диске. Некоторые мониторные программы работают с использованием протокола SNMP, например, reboot.monitor и process.monitor.

Система MON имеет такую архитектуру, что при необходимости можно создать собственный монитор. Важно, чтобы написанный нами монитор передавал основному процессу значения, которые демон может корректно обработать. Это позволяет расширять возможности системы MON в тех направлениях, которые для нас особенно важны.

Результаты проверок и действия основного процесса фиксируются в журнале системы. Также в журнал записываются ошибки, произошедшие в процессе работы системы MON.

3. Расширение системы MON

Для расширения функциональности системы MON было создано несколько дополнительных модулей. С их помощью ведется более

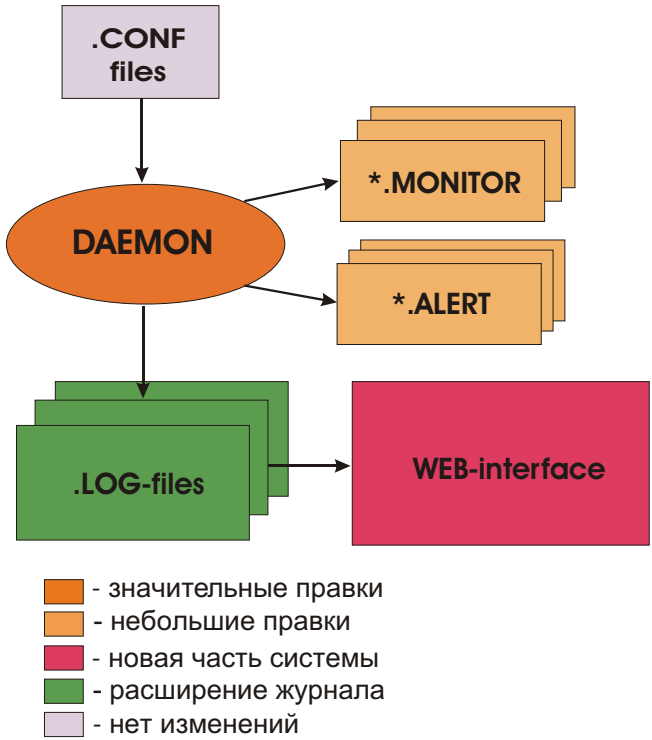

Рис. 2. Архитектура системы MON

полный журнал системы MON, генерируются данные в специальном формате для отображения состояния сети в Web, а также производятся некоторые вспомогательные действия (например, приведение даты и времени к определенному виду). Рассматриваемые модули могут использоваться как мониторными программами, так и основным процессом.

3.1. Расширение журнала системы. В оригинальной версии системы MON некоторые действия и результаты работы системы фиксировались в файле /var/log/syslog. Однако, этого оказалось мало для достижения желаемого функционирования системы MON.

Было решено вести дополнительные записи для последующего их использования при построении сайта состояния сервисов и всей сети в целом. Для этого был создан модуль Write_Log.pm

Принцип работы модуля Write_Log.pm прост: получая результат работы мониторов, он выделяет необходимую информацию и записывает эти данные в log-файл, соответствующий проверяемому сервису. В log-файле также фиксируется время проведенной проверки и название группы, которая была проверена. Все необходимые данные модуль выделяет из текстовой части, возвращенной мониторной программой. Особенным образом обрабатывается выход fping-монитора, так как он предоставляет более подробную информацию о состоянии компьютеров, чем мониторы других сервисов. Большинство мониторных программ сообщают, что сервис на данном компьютере работает, либо не работает, тогда как fping-монитор указывает качество работы сервиса, а именно процент потерянних при проверке пакетов. Вызов модуля производится в основном процессе.

3.2. Создание нового Web-интерфейса. Создание информативного Web-интерфейса для системы мониторинга позволяет постоянно следить за состояние отдельных сервисов и сети в целом. Наглядное представление удобно для восприятия и анализа. Мониторная система MON имеет некоторый Web-интерфейс, однако он не является достаточно подробным, особенно после внесения изменений в мониторные программы. Модификация мониторных программ позволила повысить качество и точность проверки, а значит увеличила количество информации о ходе и результатах проверок.

Модуль All_Stat.pm предназначен для разбора log-файлов и формирования данных в нужном формате для последующего отображения их в Web. Вызов модуля All_Stat.pm производится из основного процесса по окончании всех действий, необходимых для проведения проверки. Формирование новых данных происходит с некоторой периодичностью. Период определяется как минимальный интервал между проверками среди всех интервалов, заданных в конфигурационном файле. Основными задачами модуля являются:

(1) разбор log-файлов с целью определения состояния каждого компьютера в каждый момент времени;
(2) отнесение каждого компьютера к определенной группе;
(3) разделение данных, относящихся к разным сервисам;

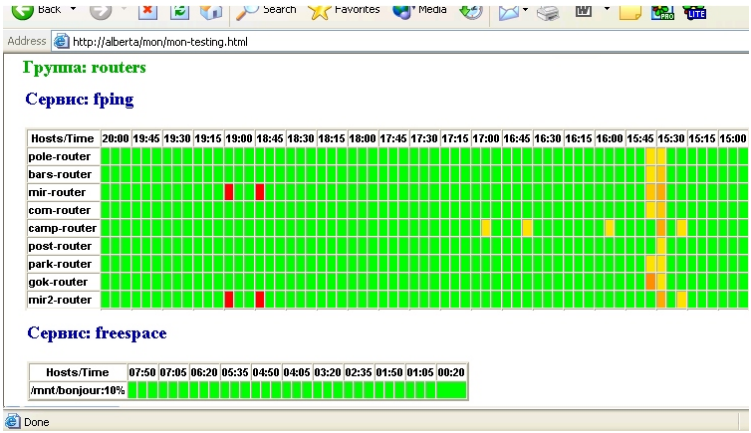

Рис. 3. Новый Web-интерфейс системы MON

(4) формирование данных для скриптов, осуществляющих отображение собранной в браузере информации.

В результате модуль All_Stat.pm создает текстовый файл определенного формата, в котором записано состояние каждого компьютера из группы по всем сервисам после всех проверок, произведенных за текущие сутки. Полученный файл используется JavaScript-программами для отображения в Web.

Состояние сети представлено в Web в виде таблицы. Перед таблицей указано, к какой группе и сервису она относится. В столбцах указано время проверок, в строках — названия проверяемых компьютеров. На пересечении стоки и столбца можно увидеть состояние интересующего компьютера в определенный момент времени. Состояние отображается цветом. Считается, что работоспособный сервис отображен зеленым цветом, неработоспособный — красным. Цвет клетки вычисляется специальной функцией в зависимости от степени доступности сервиса. Шкала используемых цветов изображается перед таблицей и представляет собой градиентный переход от зеленого к красному.

Важной особенностью сайта является то, что построение таблицы происходит на стороне клиента. Сервер только предоставляет исходные данные в текстовом виде, тогда как на клиентской машине средствами JavaScript строится цветовое изображение (Рис. 3).

Предполагается ввести некоторую оптимизацию во внешний вид сайта. Она будет заключаться в том, что если в течение какого-либо промежутка времени все компьютеры в группе находились в одинаковом состоянии, то отображать не каждую проверку в одной клетке, а нарисовать всего одну клетку таблицы и указать соответствующий интервал времени.

4. Изменения, внесенные в систему MON

Для того чтобы сделать процесс наблюдения за работой сети более качественным и удобным, было принято решение внести изменения в систему мониторинга MON. Результатом этих модификаций прежде всего являются:

(1) оповещение в случае восстановления части компьютеров проверяемой группы;
(2) возможность построения Web-сайта состояния сети на основе данных, полученных от мониторов в ходе проверок;
(3) изменение параметров проверок для повышения точности результата.

Для совершения перечисленных действий используются модули, описанные в главе 3.

4.1. Модификация мониторов. Код мониторных программ подвергся минимальным изменениям. Каждая мониторная программа выполняет отведенную ей функцию, а именно проверку конкретного сервиса, тогда как основной процесс занимается организацией всего процесса и обработкой полученных результатов. Было принято решение не увеличивать функциональность мониторных программ, но при этом изменить “восприятие” основным процессом полученных результатов.

Некоторые изменения были внесены в мониторную программу, проверяющую доступность компьютеров с помощью утилиты ping, fping.monitor. Для повышения точности проверки введена возможность передачи монитору дополнительных параметров, таких как количество и размер посылаемых пакетов, время между посылкой пакетов. Важным параметром среди добавленных является количество допустимых потерь пакетов при проверке. Введение этих изменений с соответствующей обработкой позволяет точнее узнать состояние проверяемого компьютера. До внесения перечисленных изменений мониторная программа могла различить компьютеры на доступные и

недоступные. После внесения возможности использования дополнительных параметров проверки стало возможным определять частичную доступность хостов, что помогает оценить не только работоспособность сети, но и качество ее работы.

4.2. Изменения, внесенные в основной процесс мониторной системы. Основные изменения главного процесса мониторной системы MON затронули процедуру, занимающуюся обработкой значений, полученных от мониторных программ. Именно в ней принимается решение о посылке сообщения о некотором событии в сети.

Одним из недостатков оригинальной версии системы MON является то, что система не может присылать оповещение персоналу в случае восстановления части ранее недоступных компьютеров при проверке определенного сервиса. Это означает, что если N компьютеров были сломаны, а затем K компьютеров восстановились (где K<N), персонал не узнает о восстановлении подгруппы до тех пор, пока остальные N-K компьютеров не будут также введены в строй. Это связано с тем, что возвращенные мониторами значения демон интерпретирует только двумя способами — полностью успешная проверка или полностью провальная проверка.

Для того чтобы стало возможным оповещение в случае восстановления части группы, была расширена соответствующая функция основного процесса. В текстовой части о результатах проверки, полученной демоном от мониторной программы, имеется строка, в которой перечислены машины, непрошедшие последнюю проверку. При этом основной процесс хранит в памяти такую же строку, полученную при предыдущей проверке. Очевидно, что для каждой группы хостов и для каждого сервиса имеются свои данные (своя строка). Написав функцию сравнения соответствующих строк, можно выделить те машины, которые восстановились, а также обнаружить поломку других членов группы, если таковая имеется. После этой процедуры демон принимает решение о посылке письма, в котором сообщает о компьютерах, которые восстановлены, либо о тех, которые добавились в список сломанных.

Кроме того, были добавлены дополнительные проверки для счетчиков, которые следят за тем, чтобы не было послано лишних сообщений о поломке, а также несколько константных значений, используемых для определения типа сообщения демоном. В этом возникла необходимость, так как после совершения посылки сообщения о

восстановлении лишь части компьютеров, основной процесс считал, что послано сообщение о полном восстановлении и посылал новое сообщение о поломке. Дополнительная проверка позволила избежать отправления избыточных сообщений.

Небольшим добавлением в основной процесс можно считать вызов функции построения структуры данных для создания Web-сайта.

Значительным изменением основного процесса было вынесение парсера конфигурационного файла в отдельный модуль. При построении данных для Web-сайта используется не только информация из log-файлов, но и основная конфигурация работы системы. Это означает, что мониторным программам необходимо производить разбор конфигурационного файла. Чтобы избежать повторения кода, соответствующая функция была вынесена в отдельный модуль.

5. Выводы

В результате проделанной работы получена мониторная система, удовлетворяющая требованиям персонала СТ «Ботик». Система MON сейчас тестирует доступность роутеров, некоторых серверов, а также различные сервисы, где это необходимо. Дальнейшее развитие системы MON позволит максимально ее усовершенствовать и благодаря ей оптимизировать работу обслуживающего персонала.

Благодарности. Автор благодарен Ю. В. Шевчуку за проведенные консультации и плодотворные обсуждения по теме работы, а также С. М. Абрамову за конструктивные предложения и помощь при подготовке статьи. Идеи, высказанные П. Г. Жбановым, были использованы при реализации частей работы, описанные в главе 3. Особая благодарность С. В. Бурчу за участие в тестировании полученного продукта.

Список литературы

[1] Кристиансен Т., Торкингтон Н. PERL: библиотека программиста: Издание официальное. — СПб: Питер, 2001. ↑

[2] Шевчук Ю. В.. 1999. *Методы построения экономически эффективных региональных компьютерных сетей*, Диссертация на соискание степени кандидата технических наук, Институт программных систем РАН, Переславль-Залесский. ↑

[3] Абрамов С. М., Пономарев А. Ю., Шевчук Ю. В.. 1999. *Широко доступный Интернет как путь в открытое общество. Опыт Переславля-Залесского*, Труды конференции "Интернет. Общество. Личность", СПб. ↑

[4] Абрамов С. М., Пономарев А. Ю., Шевчук Ю. В.. 1999. *Технология построения недорогих, но качественных гражданских сетей. Опыт Переславля и его перенос в другие регионы*, Тезисы докладов Всероссийской научной конференции "Научный сервис в сети Интернет", МГУ. ↑

[5] Абрамов С. М., Позлевич Р. В., Пономарев А. Ю., Шевчук Ю. В.. 1997. *Экономически эффективные технологии построения региональных сетей для науки и высшей школы*, Труды конференции Телематика'97, СПб. ↑

[6] *Сеть для всех и по разумным ценам* // Компьютерра, № 34, с. 28 – 30. (russian) ↑

Исследовательский центр мультипроцессорных систем, лаборатория «Ботик» ИПС РАН

V. V. Parmyonova. *Adaptation of monitoring system MON for telecommunication laboratory "Botik".* (in russian.)

Abstract. Telecommunication Laboratory "Botik" uses monitoring system MON to control the network in Pereslavl-Zalessky. Mon is free software, that is why it can be changed for better functioning. This report shows the additions and modifications to MON, such as improvement the alerting system, creation of new WEB-interface and increase of tests quality.