

МОНИТОРИНГ СЕТЕВЫХ УСТРОЙСТВ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Шульга А.В.

Мельниченко Д.А. – к.т.н., доцент

Основной задачей системного администратора в организации является поддержание сетевого оборудования в рабочем состоянии, что подразумевает постоянный мониторинг хостов – устройств, имеющих сетевой интерфейс и подключенных к локальной сети (ПК, сервер, коммутатор, сетевой принтер).

Мониторинг хостов это периодическая проверка работоспособности тех или иных служб, портов и протоколов. Наиболее распространенный способ – отправка специальных ICMP-запросов и ожидание ответа на них (пинг). Один из критических параметров мониторинга – время отклика устройства. Оно позволяет оценить загруженность самого устройства и каналов связи. Способы мониторинга хостов зависят от задач, выполняемых самим устройством. Например, к web-серверу применяется проверка работы http-протокола, к коммутатору – считывание и анализ параметров по протоколу SNMP и т.д [1].

Мониторинг в локальной сети предназначен для контроля над количеством подключенных к ней устройств, работоспособностью служб и сбора информации о среднесуточной и пиковой нагрузке. Эти данные необходимы системному администратору для своевременной и быстрой реакции на сбои в работе хостов, для оптимизации работы оборудования исходя из значений измеренных «пиков», а так же для планирования и проведения модернизации локальной сети в связи с увеличением нагрузки.

Существуют серверные и клиент-серверные решения для мониторинга хостов. Как правило, серверное сканирование осуществляется с помощью периодического опроса всего диапазона IP-адресов в сети, что показывает все подключенные сетевые устройства. Подобное сканирование обычно повторяется раз в 5-10 минут, что позволяет собирать актуальную информацию и не сильно загружать сеть спамом из незначимых запросов. Второй тип серверного мониторинга хостов – считывание кэша ARP-таблиц сетевых маршрутизаторов. Этот метод быстрее первого и не требует множества запросов, которые могут приобретать существенные объемы при большом размере сети. Но его главным недостатком является невозможность обнаружения подключенных хостов, которые при этом не проявляют никакой сетевой активности.

В отличие от серверных методов мониторинга хостов, которые дают крайне ограниченное количество информации, клиент-серверные решения могут постоянно считывать большое количество параметров компьютера и пересылать их для анализа серверу. Главный плюс такого мониторинга хостов – возможность построения отказоустойчивой системы с повторным опросом клиента в случае отсутствия данных от него в течение определенного промежутка времени и автоматическим генерированием сигнала тревоги. Кроме информации о наличии устройства в сети, клиент-серверное решение мониторинга хостов контролирует запущенные на удаленном компьютере службы, правильность работы протоколов, открытые порты и многое другое. При этом коммутаторы и принтеры опрашиваются посредством все тех же ARP-запросов или пинга. Общим недостатком всех клиент-серверных методов мониторинга хостов является дополнительная нагрузка на ПК, более всего на оперативную память, которая может быть ощутима на слабых машинах, особенно совместно с другими приложениями для контроля других параметров компьютера [2].

Современные программы мониторинга обладают необходимыми механизмами визуализации и построения статистических отчетов. В качестве визуальных средств отображения данных могут быть использованы графики, диаграммы, графы сетей и подсетей и т.д. Наиболее известными программами мониторинга с открытым кодом (бесплатные) являются: ZABBIX, Nagios, Total Network Monitor, Dude.

Системному администратору необходимо проводить мониторинг на регулярной основе, т.к. данная процедура позволит:

1) Снизить производственные затраты в сфере IT. Мониторинг хостов минимизирует время выявления неполадки, т.е. позволяет экономить средства.

2) Повысить производительность работы. Вариант автоматического мониторинга хостов позволяет отступить от привычной для кого-то ручной проверки работоспособности сетевых устройств. Это позволяет системному администратору экономить время и затрачивать его на более важные проблемы.

3) Повышение лояльности клиентов. Пользователь обычно отказывается от использования услуг не вследствие единичного негативного опыта работы с сервисом, а из-за постоянных сбоев в работе. Поэтому важно в минимальные сроки устранять не только крупные поломки, но и незначительные простои, повышая стабильность системы и «процент доверия» клиентов компании.

4) Планировать обновления инфраструктуры сети с целью увеличения пропускной способности сети. При постоянном мониторинге, используя время отклика хостов, можно выявить узкие места в сети, локализовать подверженное частым сбоям оборудование и своевременно его заменить [1].

Мониторинг помогает обеспечить предупреждение и своевременное реагирование на неполадки сетевого оборудования, позволяет экономить время и защищает от потери прибыли и клиентов.

Список использованных источников:

1. http://50rus.info/articles_ru/everything_else/непрерывный-мониторинг-хостов-в-сети/
2. <http://www.rusarticles.com/programmy-statya/nepreryvnyj-monitoring-xostov-v-seti-5372296.html>