**Технологии мониторинга компьютерных сетей**

В последние годы информационные технологии претерпевают значительные и постоянные изменения. По некоторым оценкам, за последние пять лет объем сетевого трафика локальных сетей вырос в десять раз. Таким образом, локальные сети должны обеспечивать все большую пропускную способность и необходимый уровень качества обслуживания. Однако какие бы ресурсы ни имела сеть, они все-таки конечны, поэтому для сети необходима возможность управления трафиком.

А для того чтобы управление было максимально эффективным, требуется возможность контроля над пакетами, передающимися между устройствами вашей сети. Также у администратора существует великое множество обязательных для исполнения ежедневных операций. Это, например, проверка правильности функционирования электронной почты, просмотр регистрационных файлов на предмет выявления ранних признаков неисправностей, контроль за подключением локальных сетей и за наличием системных ресурсов. И здесь на помощь могут прийти средства, применяемые для мониторинга и анализа вычислительных сетей.

Чтобы не запутаться в многообразии методик, средств и продуктов, созданных для мониторинга, начнем с краткого описания нескольких крупных классов этих продуктов.

Системы управления сетью (Network Management Systems). Это централизованные программные системы, которые собирают данные о состоянии узлов и коммуникационных устройств сети, а также о трафике, циркулирующем в сети. Эти системы не только осуществляют мониторинг и анализ сети, но и выполняют в автоматическом или полуавтоматическом режиме действия по управлению сетью — включение и отключение портов устройств, изменение параметров мостов адресных таблиц мостов, коммутаторов и маршрутизаторов и т.п.

Средства управления системой (System Management). Средства управления системой часто выполняют функции, аналогичные функциям систем управления, но по отношению к другим объектам. В первом случае объектом управления является программное и аппаратное обеспечение компьютеров сети, а во втором — коммуникационное оборудование. Вместе с тем некоторые функции этих двух видов систем управления могут дублироваться, например средства управления системой могут выполнять простейший анализ сетевого трафика.

Встроенные системы диагностики и управления (Embedded systems). Эти системы выполняются в виде программно-аппаратных модулей, устанавливаемых в коммуникационное оборудование, а также в виде программных модулей, встроенных в операционные системы. Они выполняют функции диагностики и управления только одним устройством, и в этом их основное отличие от централизованных систем управления.

Анализаторы протоколов (Protocol analyzers). Представляют собой программные или аппаратно-программные системы, которые ограничиваются, в отличие от систем управления, лишь функциями мониторинга и анализа трафика в сетях. Хороший анализатор протоколов может захватывать и декодировать пакеты большого количества применяемых в сетях протоколов — обычно несколько десятков. Анализаторы протоколов позволяют установить некоторые логические условия для захвата отдельных пакетов и выполняют полное декодирование захваченных пакетов, то есть показывают в удобной для специалиста форме вложенность пакетов протоколов разных уровней друг в друга с расшифровкой содержания отдельных полей каждого пакета.

Экспертные системы. Системы этого вида аккумулируют человеческие знания о выявлении причин аномальной работы сетей и возможных способах приведения сети в работоспособное состояние. Экспертные системы часто реализуются в виде отдельных подсистем различных средств мониторинга и анализа сетей: систем управления сетями, анализаторов протоколов, сетевых анализаторов. Простейшим вариантом экспертной системы является контекстно-зависимая help-система. Более сложные экспертные системы представляют собой так называемые базы знаний, обладающие элементами искусственного интеллекта.

Многофункциональные устройства анализа и диагностики. В последние годы в связи с повсеместным распространением локальных сетей возникла необходимость разработки недорогих портативных приборов, совмещающих функции нескольких устройств: анализаторов протоколов, кабельных сканеров и даже некоторых возможностей ПО сетевого управления.

Мониторинг хостов и сетевых служб

Кроме визуального наблюдения за состоянием сетевых устройств, программное обеспечение дает возможность организации проверки хостов и служб (в том числе и локальных ресурсов или интернет-серверов) с помощью разнообразных сетевых протоколов настройки и использования удобного способа оповещения системных администраторов о положительных или отрицательных результатах тестирования. Способы могут быть разными: появление сообщения на экране компьютера ИТ специалиста, специальный звук, отправка электронного письма или смс на телефон. Приложение для мониторинга компьютеров в локальной сети предприятия в ряде случаев может перезапустить какую-либо удаленную службу либо выполнить заранее написанный для него скрипт (тогда некоторые сбои будут устраняться в автоматическом режиме).

Если в программе реализована такая функция, то все подключенные к сети устройства будут наглядно отображаться на ее схеме. Уже по одному виду их иконок специалисту станет понятно, какие из них работают нормально, а какие функционируют неверно. Такая возможность облегчает диагностику групповых сбоев. Полученные результаты тестирования заносятся в единую базу данных; по мере накопления статистической информации можно будет строить графики, чтобы изучать изменение отклика устройств и отслеживать другие проверяемые параметры.

Современные программы мониторинга компьютеров в локальной сети позволяют создать своего рода пульт управления сетевой инфраструктурой предприятия, при помощи которого отвечающий за сеть сотрудник сможет как наблюдать за ее важными элементами и проверять параметры оборудования, так и вести эффективное управление удаленными хостами. С помощью контекстного меню хостов можно просматривать различные данные об удаленных узлах в сети: проверять информацию по SNMP с коммутаторов, получить доступ к реестрам удаленных компьютеров, просматривать запущенные процессы и журналы событий, производить перезапуск служб и выполнять другие действия.

Некоторые программы ведут не только мониторинг ресурсов компьютера, но и помогают проводить учет устройств и программных приложений на сетевых ПК. Благодаря им системный администратор имеет возможность получать практически любые сведения об аппаратном и программном обеспечении на компьютерах в корпоративной сети. Сбор данных проходит удаленно, это позволяет не мешать работать сотрудникам предприятия, и экономит рабочее время системных администраторов.

Мониторинг компьютерного «железа»

Программы наблюдения за ПК в локальной сети позволяют вести точный учет аппаратного обеспечения. ИТ специалисты смогут оперативно узнать о пропаже и неисправности какого-либо компонента либо о его замене. При обнаружении изменений они заносятся в журнал, и о них оповещается администратор сети. Если нужно отслеживать определенные параметры на рабочих станциях пользователей с конкретной частотой и получать оповещения при их изменении, возможно будет настроить сбор данных по расписанию. В этом случае мониторинг ресурсов компьютера будет вестись в автоматическом режиме.

Мониторинг компьютерного «железа»

Многие программы не только формируют отчеты по компонентам компьютеров, но и следят за их работоспособностью – контролируется функционирование жестких дисков и их температура. Когда какой-либо диск перегревается или приложение выдает прогноз о том, что он может выйти из строя, сисадмин увидит отчет, содержащий критические замечания по работе ПК с предупреждением.

Учет ПО и лицензий

При необходимости софт мониторинга ПО в локальных сетях предприятия позволяет отслеживать и изменения в установленных программах. В случае, когда права пользователей строго не ограничиваются, кто-либо из сотрудников предприятия может установить на своем компьютере нежелательное или нелицензионное приложение. При мониторинге, когда происходит инсталляция или удаление программного обеспечения, любое изменение фиксируется и заносится в журнал. Это означает, что системный администратор будет всегда знать, какие именно программы и куда были инсталлированы или откуда удалены.

Часто при мониторинге ресурсов компьютера происходит отслеживание серийных номеров и лицензий программ, подсчет количества установок ПО, контроль правильного использования серийных номеров. Все эти меры реально помогают избежать проблем при проверке корпоративного программного обеспечения на предмет лицензионной чистоты. С целью повышения уровня безопасности и отказоустойчивости компьютеров ряд специальных программ мониторинга имеют функции просмотра проведенных обновлений ПО и системы и составления отчета по работе антивирусного софта и актуальности его баз.

Составление отчетов

Данные, собираемые программой с сетевых компьютеров и отображаемые на экране ПК системного администратора, могут быть занесены в отчет. Далее их можно распечатать или экспортировать в определенную базу. Кроме автоматически собираемой информации, многие приложения для мониторинга ресурсов компьютера разрешают вводить вручную серийные номера оборудования, номера офисов их пользователей и их контактные данные.