СОВРЕМЕННЫЕ СРЕДСТВА МОНИТОРИНГА СЕТИ

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

Семянович В.А.

Мельниченко Д.А. – к.т.н., доцент

Сбои в работе сетевого оборудования часто приводят к простою всего рабочего процесса, что чревато финансовыми потерями. Чтобы своевременно устранять неполадки в работе сетевых устройств (компьютер, коммутатор, сервер, сетевой принтер) необходимо вовремя их диагностировать. Непрерывный мониторинг сети – обязательная часть работы администратора, которая помогает решить множество проблем, связанных с сетью и сетевыми устройствами.

Для осуществления постоянного наблюдения за сетью на компьютер администратора или сервер устанавливается программа мониторинга сети, которая сканирует сеть и выявляет все имеющиеся в ней устройства. Таким образом, администратор освобождается от необходимости самостоятельно составлять список хостов, входящих в сеть. Опрос хостов должен происходить удаленно, чтобы не прерывать рабочий процесс. В программе мониторинга сети поддерживаются наборы проверок, с помощью которых системный администратор может вовремя узнать о любых неполадках в сети и максимально быстро их устранить [1].

Прежде всего, программа для мониторинга сети должна иметь возможность непрерывно проверять подключения к различным портам устройств по протоколу TCP/IP. Таким образом, проверяется доступность и состояние сервера или любого другого хоста в сети. Периодически опрашивая, например, TCP-порт, можно вовремя узнать о прекращении работы того или иного устройства, не сходя с рабочего места. Это позволяет системному администратору оперативно реагировать и вовремя устранять возникшие неполадки. Также, с помощью мониторинга определенных TCP-портов можно своевременно обнаруживать вредоносное программное обеспечение. При настройке проверок определенных портов, программа для мониторинга сети должна оповещать администратора в случае открытия какого-либо порта из отслеживаемого диапазона портов (список портов, используемых вредоносными программами, можно найти в Интернете).

Очень важен мониторинг устройств через ARP и NetBIOS протоколы. Через них можно контролировать изменения MAC-адресов для предотвращения несанкционированного подключения к корпоративной сети. Если знать MAC-адрес определенного хоста с определенным IP-адресом, то изменение первого может свидетельствовать о неполадках в устройстве или в его работе, а также о попытке подключиться к сети без разрешения администратора.

Для владельцев веб-сайтов необходим постоянный мониторинг HTTP-сервера и содержимого веб-страниц. Программа для мониторинга сети должна позволять вовремя узнавать о неполадках на веб-сервере и об изменении содержимого веб-страниц, содержащихся на нем. Это даст им возможность обезопасить себя от случаев несанкционированного изменения веб-страниц в случае взлома сервера злоумышленниками [2].

Проверка запущенных на удаленных компьютерах процессов необходима по многим причинам. Во-первых, она помогает в обнаружении на удаленных машинах вредоносного программного обеспечения – в этом случае нужно заранее знать имена процессов, запускаемых вирусами. Во-вторых, такая проверка позволяет администратору контролировать действия пользователей, запускающих определенные приложения в рабочее время, такие как: игры, медиа-проигрыватели и т.д.

Контроль размеров файлов и папок необходим любой компании, поскольку журналы некоторых программ входе работы могут разрастаться до невероятных размеров, занимая место на жестком диске локального компьютера, сервера или базы дынных, мешая тем самым нормальной работе сотрудников. Поэтому данная проверка также должна осуществляться программой для мониторинга сети.

Постоянный мониторинг работы различных сетевых устройств позволяет администратору вести собственную статистику, например, времени отклика хостов. Чем выше это время, тем выше загруженность устройства. Таким образом, он может узнать, к примеру, дни наибольшей загруженности сервера, и заранее подготовиться к возможным перегрузкам и сбоям в работе, чтобы вовремя их устранить [1].

Помимо всего прочего в программе для мониторинга сети должен быть предусмотрен широкий список оповещений администратора о возможных неполадках: отображение сообщений на экран, отправка сообщения на e-mail, звуковое оповещение, отправка SMS, выполнение VB и JS-скриптов. А также должна иметься возможность настройки реакции программы на определенные результаты мониторинга, например, запуск внешней программы с параметрами; запуск, останов или перезапуск службы; перезагрузка, включение, выключение удаленного компьютера. Все это должно значительно облегчить работу администратора и повысить эффективность мониторинга сетевых устройств и компьютеров [2].

Мониторинг сети – поиск медленных или неисправных систем – одна из важнейших задач сетевого администратора. Можно без преувеличения сказать, что от успешности решения этой проблемы во многом зависит работоспособность всего предприятия в целом. Задача программы для мониторинга сети – сделать процесс мониторинга более эффективным за счет широкого спектра проверок сетевых устройств.

Список использованных источников:
1. http://www.good-article.ru/articles/1010432.html
2. http://www.rusarticles.com/programmy-statya/programma-monitoringa-seti-3142699.html