**Сетевой мониторинг от Ipswitch**

Михаил Брод

Управление большими сетями - занятие сложное, требующее много сил и времени. Системному администратору приходится решать большое количество вопросов - отслеживать конфигурацию сети, проводить поиск "узких" мест, тестировать установленные в сети устройства, да мало ли еще какие задачи возникают в процессе работы. Неудивительно, что для администратора создаются специальные системы, призванные облегчить и упростить его работу, выполнять рутинные задачи в автоматическом режиме, информирующие его о всех возникающих в сети коллизиях.

Компания Ipswitch, Inc. недавно представила обновленный вариант своего продукта Ipswitch WhatsUp Professional, предназначенного для сетевого мониторинга в небольших и средних предприятиях. Программа позволяет обнаруживать сетевые устройства, инициировать их мониторинг, выполнять действия, основанные на изменении их статуса, что дает возможность идентифицировать отказы до того, как они становятся катастрофическими.

Программа Ipswitch WhatsUp Professional использует различные способы проверки состояния установленных в сети сервисов. В зависимости от типа поддерживаемых ими протоколов, используется соответствующий способ опроса и определения текущего статуса. По умолчанию используется самый простой способ проверки - пингование (ping) сетевых устройств с использованием протокола ICMP. Чем он привлекателен - тем, что он крайне мало влияет на общесетевой трафик (а если сеть большая, то любое увеличение трафика будет сказываться на общей производительности). Но есть и обратная сторона - проверка таким способом обеспечивает лишь получение информации о том, присутствует ли исследуемое устройство в сети (отвечает ли оно) или нет. В зависимости от ответа, могут выполняться определенные в программе действия.

При первом запуске программы формируется список найденных в локальной сети устройств. Их можно идентифицировать либо IP-адресами, либо именем хоста. В настройках каждого устройства можно указать индивидуально, как его показывать в списке, с какой периодичностью выполнять проверку, тип проверки (используемый протокол - кроме ICMP можно использовать IPX или NetBios). Для одного и того же хоста можно назначить несколько проверяемых сервисов (или выбрать один из доступных), в том числе проверку FTP, HTTP, IMAP4, POP3 и других сервисов. Для каждого из устройств можно установить особые периоды проверки в течении любого из дней недели, установив периоды, когда такая проверка будет выполняться вне зависимости от иных настроек. Проверку сетевого устройства также можно увязать с событиями, связанными с иными сетевыми устройствами. Имеется два варианта настроек - либо проверять, когда другое устройство находится в рабочем состоянии, либо наоборот, когда оно недоступно. Например, если проверяемое устройство находится относительно компьютера с установленной программой Ipswitch за роутером, то проверять его имеет смысл только в том случае, если роутер находится в рабочем состоянии.

Для проверки сетевых устройств и сервисов предусмотрено два режима мониторинга - активный и пассивный. Тот режим, что принимается по умолчанию - пингование - относится к активному режиму, поскольку его инициирует программа. В дополнение к базовой проверке можно добавить свою. При выборе для мониторинга стандартных сервисов, программа может сама определить параметры мониторинга. Но если у вас установлен нестандартный сервис или устройство, придется самостоятельно описывать команды. Для этого используется специальный редактор для написания скриптов. Например, для проверки сервиса IRC можно ввести и использовать такой скрипт:

Name: IRC; Port: 6667; TCP.

Send=Version/r/n

Expect=irc

Send=QUIT/r/n

Но не все сетевые сервисы могут отвечать на посылаемые им запросы об их состоянии. Например, не будет ответа от антивирусного сервиса, который сам формирует сообщения при обнаружении вирусных атак. Для отслеживания таких сервисов используется пассивный режим. Программа поддерживает три различных варианта настройки пассивного мониторинга. SNMP-монитор прослушивает различные устройства, например, сетевые принтеры для получения информации об отсутствии в них бумаги. Syslog monitor применяют для отслеживания сообщений, содержащих определенные ключевые слова и помещаемые в файлы системных логов различными устройствами или сервисами, в основном запущенных на компьютерах под управлением Unix. Windows Event Log Monitor проверяет записи о событиях, фиксируемых в системных логах Windows. Например, если на компьютере установлен Norton AntiVirus, то для получения информации о его работе может быть включен монитор следующего типа:

Display Name Virus Scan

Source Norton AntiVirus

Type Any

Event ID 4098

Match On ~completed

При изменении статуса того или иного подконтрольного объекта, программа Ipswitch WhatsUp Professional может запускать выполнение тех или иных действий. Действия могут быть как глобальные, распространяемые на изменения статусов любых устройств, так и индивидуальные. При разработке политики выполнения тех или иных действий нужно учитывать, что может произойти, например, в случае остановки работы роутера - одновременно отключится большое количество компьютеров, что приведет к появлению сигнала об изменении их статуса. И здесь нужно учитывать зависимости устройств, чтобы не множить рассылаемые сообщения. Результирующие действия могут оформляться в виде подачи звуковых сигналов, отправки сообщений на пейджер, SMS, e-mail, попытки перезапуска сервиса или запуска дополнительной программы, записи сообщения в системный лог-файл, выполнения иных действий.

Для удобства просмотра устройств, состава и структуры сети, в программе предусмотрена возможность визуализации имеющихся устройств и их взаимосвязи. Первоначальный обзор сети, выполняемых при первом запуске программы, формирует список сетевых устройств. В этом списке отображаются адреса устройств, их наименования, здесь же можно ввести их описания. Устройства можно располагать по группам, подсетям, по иным параметрам, создавать на них ссылки из одной группы в другую. Эти данные сохраняются в базе данных и в дальнейшем выбираются из нее. При необходимости можно выполнять обновление, добавление устройств как путем их поиска, так и ручным добавлением.

После формирования списка локальной сети, у меня все найденные устройства были определены как рабочие станции, независимо от того, были ли это рабочие компьютеры, сервера, маршрутизаторы. В таком виде информация о составе и структуре сети не представляет большого интереса. Но можно определить тип устройства вручную - по типу оборудования, по типу установленной операционки. Изменение типа отразится на том, какой иконкой он будет отображен на карте локальной сети. Карта сети - это второй, графический вариант отображения состава и структуры сети. На карте великолепно визуализируются связи и соединения различных сетевых устройств, различным цветом отображаются включенный и отключенные устройства и сервисы. На карте можно вводить связи, используемые для анализа взаимодействия интерфейсов различных устройств, создавать и выделять группы.

При исследовании сети можно задавать дополнительные условия - каким протоколом выполнять поиск, какого типа устройства включать в число обнаруженных. Создаваемый подобным образом список устройств можно сохранить под отдельным именем и их мониторинг вести независимо от остальных устройств.

Как и иные программы, ведущие наблюдение за состоянием объектов, программа Ipswitch WhatsUp Professional может формировать разнообразные отчеты, основанные на полученных данных. Можно выделить несколько базовых типов отчетов. Это - отчет о работоспособности устройств, отчет о выполненных действиях, отчет об обработанных сообщениях SNMP, отчет о событиях в системных логах и логах Windows. В отчете о действиях будут показаны все назначенные включенным в отчет устройствам действия и то, были ли они когда-либо активированы или нет. Отчеты могут быть сформированы как в целом по локальной сети, так и по отдельным устройствам или группам.

К программе можно получить доступ и через веб-интерфейс, если такая опция включена в настройках. По умолчанию есть два пользователя - admin и guest с соответствующими паролями. Но могут быть созданы и учетные записи других пользователей. Помимо доступа по обычному протоколу, можно задействовать защищенный протокол с поддержкой SSL. Это обеспечит определенную безопасность передаваемых данных. Для удобства администратора есть возможность включить работу утилиты, размещаемой в панели задач. Цвет, отображаемый на ней, показывает отсутствие или наличие каких-либо проблем в контролируемой программой сети.

Программа Ipswitch WhatsUp Professional прекрасно справляется с задачей наблюдения за режимом работы сети и сетевых устройств. Но не следует думать, что она же поможет решать и возникающие проблемы - это уже не ее задача.