ВНЕДРЕНИЕ СИСТЕМЫ МОНИТОРИНГА ДЛЯ ОБЕСПЕЧЕНИЯ НАДЕЖНОСТИ РАБОТЫ КОМПЬЮТЕРНОЙ СЕТИ ПРЕДПРИЯТИЯ ООО «АСПЕКТ ПРИМОРЬЯ» Г. ВЛАДИВОСТОК

Слесаренко Александр Александрович
Владивостокский государственный университет экономики и сервиса, г. Владивосток.

Актуальность рассматриваемого вопроса состоит в том, что одно из основных приложений для наблюдения за таким важным показателем, как надежность работы сети во время ее эксплуатации - это системы мониторинга и управления NMS (Network Management System). При внедрении системы NMS, у операторов появляется возможность использования комплексного решения с способностью получить доступ в реальном времени работы к контролю выбираемых параметров оборудования, которое установлено в сети, и их архивизирование, а также анализ всей собранной информации.

Однако проблема заключается в том, что на протяжении долгого периода времени осуществлять мониторинг элементов сети было возможно только посредством применения решений закрытого типа от разных поставщиков. Базой таких решений являлись разные, несовместимые между собой протоколы. С целью внедрить мониторинг оборудования в сети различных поставщиков операторы применяли несколько не совместимых между собой систем (интерфейс SNMP использовали для коммуникации с системой управления на более высоком уровне). В свою очередь, системы управления высокого уровня – это очень дорогостоящее решение, а сама интеграция через SNMP была очень сложным процессом.

В современных условиях рынок предлагает решения открытого типа, которые позволяют одновременно применять оборудование от многих поставщиков. Поэтому остро стоит вопрос выбора такой системы мониторинга, которая бы максимально хорошо отвечала всем задачам слежения за оборудованием в компании.

Для решения указанной проблемы необходимо применить метод анализа программных продуктов, выполняющих функции мониторинга и управления сетевыми объектами. То есть на основании анализа существующих решений, а так же протоколов сетевого управления и мониторинга оборудования необходимо выбрать программный продукт с открытым исходным кодом.

В целом, выбор способов и объектов мониторинга сети находится в зависимости от таких факторов, как конфигурация сети, действующие в ней сервисы и службы, конфигурация серверов и установленного на них ПО, возможностиПО, используемого для мониторинга и т.п. На самом общем уровне можно говорить о следующих элементах:

- проверки физической доступности оборудования;
- проверки состояния (работоспособности) служб и сервисов, которые запущены в сети,

- детальной проверки не критичных, но важных параметров функционирования сети, таких как производительность, загрузка и т.п.;

- проверки параметров, специфичных для сервисов и служб данного конкретного окружения (наличие некоторых значений в таблицах БД, содержимое лог-файлов).

Способы проверки этих величин варьируются, но одним из основных, доступных почти всегда – является проверка по SNMP-протоколу.

В общем, можно отметить следующие системы мониторинга и управления.

Система управления сетью (Network Management Systems) - централизованная программная система, собирающая данные о состоянии узлов и коммуникационных устройств сети, а также данные о трафике, который циркулирует в сети. В качестве примеров такой системы управления можно привести популярные системы вроде HPOpen View, SunNetManager, IBMNetView.

Средство управления системой (System Management). Средством управления системой часто выполняются функции, которые аналогичны функциям систем управления, но по отношению к другим объектам.

Встроенная система диагностики и управления (Embedded systems).Обычно такая система выполняется в виде программно-аппаратного модуля, устанавливаемого в коммуникационное оборудование, а также в виде программного модуля, встроенного в операционные системы. В качестве примера средств данного класса можно привести модуль управления концентратором Distrebuted 5000

Анализатор протокола (Protocol analyzers). Это программная либо аппаратно-программная система, которая отграничивается в отличие от системы управления только наличием функций мониторинга и анализа трафика в сетях.

Стоит отметить, что в современных условиях организация систем управления сетями немыслима без ориентации на определенные стандарты, так как имеют сотни компаний, разрабатывающих управляющее программное обеспечение и сетевое оборудование, а, значит, и агентов для него. А поскольку, как правило, корпоративная сеть является неоднородной, то управляющими инструментами не отражается специфика одной системы либо сети.

Наиболее распространенный протокол управления сетями сегодня это протокол SNMP (Simple Network Management Protocol),который поддерживается сотнями производителей. Основные достоинства протокола SNMP заключаются в его простоте, доступности, независимости от производителей. В общем, протокол SNMP разрабатывался для того, чтобы управлять маршрутизаторами в сети Internet и выступает в качестве части стека TCP/IP.

SNMP - это протокол, который используется для того, чтобы получать от сетевых устройств информацию о таких их параметрах, как статус, производительность и характеристики, хранящиеся в специальной базе данных сетевых устройств, MIB (Management Information Base).Есть стандарты, которыми определяется структура MIB, в том числе набор типов ее переменных (объектов в

терминологии ISO), их имена и допустимые операции этими переменными (например, читать). В MIB, вместе с прочей информацией, может осуществляться хранение сетевой и/или MAC-адреса устройств. В древовидной структуре MIB содержатся обязательные (стандартные) поддеревья, а также в ней могут присутствовать частные (private) поддеревья, которые позволяют изготовителю интеллектуальных устройств реализовывать какие-либо специфические функции на основе его специфических переменных.

На сегодняшний день информационно-вычислительная сеть – это, как правило, довольно сложная, территориально распределенная и неоднородная вычислительная сеть, обеспечивающая, в первую очередь, доступ в Интернет, обмен данными, функционирование корпоративных почтовых и информационных систем, а также доступ извне к опубликованным информационным ресурсам.

В такой ситуации диагностика, поиск и устранение проблем самого различного рода, возникающих как в программных, так и в аппаратных компонентах, а также и в линиях связи, являются одними из важнейших задач для специалистов, обслуживающих ЛВС.

Nagios — является программой мониторинга компьютерных систем и сетей с открытым кодом. Её предназначение состоит в наблюдении, контроле состояния вычислительных узлов и служб, оповещении администраторов в случае, когда какими-то из служб прекращается (либо возобновляется) своя работа.

Посредством системы Nagios осуществляется мониторинг деятельности большинства сетевых сервисов: SMTP, POP3, IMAP, SSH, Telnet, FTP, HTTP, DNS и прочих. Также при помощи данного средства можно отследить использование ресурсов серверов, вроде загруженности процессора, расходования оперативной памяти, дискового пространства и т.д.

Возможно также осуществление удаленного мониторинга посредством шифрованных SSH- или SSL-туннелей. Наличие простой архитектуры модулей расширений разрешает создать свои способы проверки служб и обработчики событий. Концепция «родительских» узлов позволяет определять иерархию и зависимости между хостами. Таким образом можно найти отличия действительно неработающих узлы от недоступных системе мониторинга, которые возникли из-за неполадок на промежуточных пунктах. Важная характеристика Nagios состоит в умении строить карты сетевой инфраструктуры и графики различных параметров наблюдаемых систем.

В свою очередь Zabbix это открытое решение распределенного мониторинга корпоративного класса. Zabbix - это программное обеспечение мониторинга многочисленных параметров сети а также состояния и работоспособности серверов. Zabbix использует гибкий механизм уведомлений, что позволяет пользователям настраивать оповещения по почте практически для любого события. Это дает возможность быстро среагировать на проблемы с сервером. Zabbix предлагает отличные возможности отчетности и визуализации данных, базируясь на собранных данных. Это делает Zabbix идеальным инструментом для планирования и масштабирования.

Ещё одна система – это Munin. По сути это инструмент, который существует под *NIX (Linux, xBSD, Solaris) и Windows и позволяет централизовано отслеживать и наглядно отображать состояние подшефных систем. Изначально используется для отрисовки графиков, но также его можно использовать как чистое средство для наблюдения. Большой плюс Munin - гибкость (все графики рисуются плагинами, активными на целевых системах, и никто не запрещает использовать только те плагины, которые нужны) и возможность с одного сервера собирать информацию о множестве других. Соответственно, нагрузка на наблюдаемом сервере минимальна.

Munin является достаточно старой системой, развившейся на популярном среди администраторов средстве отрисовки графиков RRDTool. Суть идеологии RRDTool состоит в хранении данных на основании «карусельного» типа - по заполнении базы фиксированного размера RRDTool начинает затирать данные с хвоста базы (то есть со старых) к голове (к новым), чем гарантируется потеря минимального количества полезных данных, но при этом база не распухает до безумных размеров (как у HP OpenView или Zabbix). Обычно в базе RRDTool присутствуют несколько каруселей, вроде «мгновенных данных» (подлежат хранению неделю), среднего за 5 минут (генерируется на основе мгновенных данных, хранятся в течение месяца) и среднего за час (генерируются на основе 5минутных, хранятся год). Минусы RRDTool заключаются в его же плюсах. Необходимо очень внимательно рассчитать емкость базы, потому что редакция созданной базы уже невозможна, как и извлечение данных с целью переноса в другую базу - тоже. Кроме того, RRDTool отвечает только за хранение данных, а их ведь еще откуда-то надо брать.

Анализ средств мониторинга позволяет сделать заключение о том, что рациональнее реализовать потребности организации по слежению за оборудованием с помощью развертывания системы мониторинга на базе программного продукта Nagios.

Список литературы:

1 Галатенко В.А. Стандарты информационной безопасности : справочное пособие / В. А. Галатенко. – М.: Интернет- университет информационных технологий, 2014. – 328 с.

2 Донцов Д.А. Установка и настройка Windows. Легкий старт / Д.А. Донцов. – М.: Экстра, 2014. – 346 с.

3 Макарова Н.В. Информатика: Учебник для вузов / Н.В. Макарова, В.Б. Волков. - СПб: Питер, 2013. – 250 с.

4 Попов А.К. Командные файлы и сценарии Windows ScriptHost / А.К. Попов. – М.: Центр, 2012. – 453с.

5 О персональных данных: федеральный закон от 27.07.2006 № 152-ФЗ // СПС Консультант Плюс.