СИСТЕМА МОНИТОРИНГА ДЛЯ АНАЛИЗА И КОНТРОЛЯ ТРАФИКА СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

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

Петров А.Ю.

Рассмотрены вопросы обеспечения мониторинга и управления сетью передачи данных, необходимые для этого протоколы и инструменты, а также преимущества использования комплексной системы управления и мониторинга сети. В качестве системы мониторинга и отслеживания статусов различных сервисов компьютерной сети, серверов и сетевого оборудования выбрана система Zabbix, имеющая ряд преимуществ по сравнению с другими.

Целью данной работы является анализ существующих решений по обеспечению мониторинга и управления сетью передачи данных, определение оптимального решения в отношении технических параметров и затраченных ресурсов для наладки и обслуживания выбранной системы.

Для современных вычислительных сетей требуются дополнительные специальные средства управления помимо тех, которые входят в состав стандартных сетевых операционных систем. Это объясняется большим количеством различного коммуникационного оборудования, от надежности работы которого зависит работа всей сети. Распределенный характер крупной корпоративной сети делает невозможным поддержание ее работы без централизованной системы управления, которая в автоматическом режиме собирает информацию о состоянии каждого концентратора, коммутатора, мультиплексора и маршрутизатора и предоставляет эту информацию оператору сети.

Выше отмечалось, что система управления работает обычно в автоматизированном режиме – выполняет наиболее простые действия по управлению сетью автоматически, а сложные решения, на основе подготовленной информации, реализуются при участии человека.

В связи с тем, что сами системы управления представляют собой сложные программноаппаратные комплексы, существует граница целесообразности применения системы управления, которая определяется сложностью сети, разнообразием применяемого коммуникационного оборудования и степенью его распределенности по территории. Однако при росте сети может возникнуть необходимость объединения разрозненных программ управления устройствами в единую систему управления, в связи с чем, возможно, придется отказаться от этих программ и заменить их интегрированной системой управления. Для поиска оптимальной системы управления проведем сравнение систем мониторинга по следующим параметрам.

1. Формирование отчетов SLA (Service Level Agreement). Контроль гарантированных параметров качества обслуживания SLA, определяющих межоператорские взаимоотношения.

2. Формирование трендов. Выявление основных тенденций динамики показателей качества работы телекоммуникационной сети.

3. Прогнозирование трендов. Прогнозирование изменения динамики показателей качества работы телекоммуникационной сети.

4. Анализ топологии сети. Сбор информации об элементах сети.

5. Использование агентной модели мониторинга. Наличие устройств, осуществляющих сбор и передачу информации о работе сети.

6. Поддержка SNMP (Simple Network Management Protocol). Использование протокола SMNP для обмена информацией о состоянии объектов наблюдения в режиме реального времени.

7. Протоколирование событий. Формирование подробных записей о состоянии элементов сети.

8. Датчики внештатных ситуаций. Наличие устройств для оповещения о возникновении критических ситуаций, негативной тенденции к изменению показателей качества работы телекоммуникационной сети.

9. Распределенный мониторинг. Мониторинг сигнального обмена на предмет соответствия работы оборудования определенным спецификациям протоколов.

Результаты сравнительного анализа приведены в табл. 1.

Таблица 1.**Сравнительный анализ систем мониторинга**

Системы мониторинга	Параметры								
Argus									
Intellipool Network Monitor									
IPHost Network Monitor									
NetMRI									

NetQoS Performance Center									
OPNET ACE Live									
Opsview									
Scrutinizer									
Orion									
Zenoss									
Nagios									
Zabbix									

Анализ показал, что системы мониторинга, предлагаемые на мировом рынке, сходны по выполняемым функциям. Все они предоставляют почти одинаковый минимальный набор возможностей, однако каждая из них характеризуется определенными недостатками: в большинстве систем вообще не реализованы возможности прогнозирования трендов, а в системах, где они реализованы, построение происходит на основе устаревшей статистической информации. Подобное прогнозирование не учитывает фрактальность трафика, нелинейность характеристик и не стационарность процессов. Обобщив предложенные выше решения, можно синтезировать общую архитектуру системы мониторинга и управления. Все рассмотренные системы мониторинга основаны на использовании агентного подхода. Агенты собирают статистическую информацию о работе элементов сети и передают ее в центральную базу данных, затем собранная информация обрабатывается управляющими модулями. В состав системы мониторинга должны входить следующие компоненты: формирование отчетов, модуль управления SNMP, архив и консоль управления. Модуль формирования отчетов позволяет формировать из имеющихся данных информацию для принятия управленческих решений. Модуль управления SNMP отвечает за сбор информации с агентов мониторинга и взаимодействие с системами управления. Архив позволяет упорядочить хранение статистической информации и организовать последующую работу с ней. Консоль управления реализует функции конфигурирования и управления системой.

Для корпоративной сети передачи данных наиболее полезным инструментом будет протокол NetFlow, т. к. в связке с этой утилитой могут использоваться пакеты данных для представления данных в более удобном пользователю виде. По результатам анализа инструментов и средств мониторинга сделан вывод о том, что наибольшая надежность сети и наиболее эффективная передача данных обеспечиваются при использовании комплекса протоколов NetFlow и SNMP

Список использованных источников:

1. Simple Network Management Protocol (SNMP). [Электронный ресурс]. – Режим дос- тупа: http://www.ieft.org/rfc1157.txt.. – Дата доступа: 12.06.2016

2. Cecil A. A Summary of Network Traffic Monitoring and Analysis Techniques / A. Cecil [Электронный ресурс]. – Режим дос- тупа: http://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring/index.html... – Дата доступа: 13.06.2016

3. Olups R. Zabbix 1.8 Network Monitoring. [Электронный ресурс]. – Режим дос- тупа: http://www.amazon.co.uk/Zabbix-Network-Monitoring-Rihards-Olups/dp/184719768. – Дата доступа: 18.07.2016