СРАВНИТЕЛЬНАЯ ХАРАКТЕРИСТИКА ПОДХОДОВ МОНИТОРИНГА И УПРАВЛЕНИЯ КОМПЬЮТЕРНЫМИ СЕТЯМИ

С.Г. Саевич, А.П. Мателенок
Новополоцк, ПГУ имени Евфросинии Полоцкой

В настоящее время, с развитием информационных технологий, развиваются и компьютерные сети. С увеличением их масштабов, управление сетями становится сложной и трудоемкой задачей. Специалисты по сетевым технологиям ищут возможности по реализации автоматизации и упрощению части работ по управлению и наблюдению за ними.

Одна из самых горячих тем обсуждения в профессиональном сообществе – будущее протоколов мониторинга и управления сетями. Среди специалистов распространено мнение, что SNMP уходит в прошлое, а телеметрия – это путь в будущее. Этот вопрос вызывает оживленные дискуссии, поскольку затрагивает фундаментальные аспекты работы современных сетевых инфраструктур. SNMP (Simple Network Management Protocol) долгие годы служил стандартом де-факто для мониторинга и управления сетевыми устройствами, от маршрутизаторов и коммутаторов до серверов и принтеров. Однако с ростом сложности сетей и увеличением объёмов данных, которые необходимо обрабатывать в режиме реального времени, многие эксперты обратили свое внимание на телеметрию как на более современное и эффективное решение. Таким образом, **целью статьи** является анализ сильных и слабых сторон обоих подходов мониторинга и управления сетями: подхода, базирующегося на использовании SNMP, и подхода на основе использования телеметрии – а также формулировка вывода о будущем применения протокола SNMP.

Результаты и их обсуждение. SNMP работает по принципу «клиент-сервер», где клиентом выступает система управления сетью (NMS – Network Management System), а серверами – управляемые устройства с запущенными на них SNMP-агентами. SNMP собирает данные о производительности устройств с помощью механизма опроса и передаёт их на платформу управления. Доступны три версии SNMP, причём SNMPv3 добавляет важные функции аутентификации и шифрования. Администраторы сети могут использовать этот протокол для сбора данных по мере надобности.

Плюсы SNMP:

1. Простота: несмотря на свою мощь, SNMP действительно прост в использовании. Он использует всего несколько основных команд, таких как GET (получить информацию), SET (изменить настройки) и TRAP (отправить уведомление).

2. Универсальность: SNMP поддерживается практически всеми сетевыми устройствами, от домашних роутеров до промышленных коммутаторов.

3. Иерархическая структура данных: информация о параметрах устройства в SNMP организована в виде таблицы, называемой MIB (Management Information Base), в которой имена всех параметров организованы в иерархическое дерево. Каждый «лист» этого дерева – это определенный параметр устройства, имеющий уникальный идентификатор – OID (Object Identifier).

4. Эффективность: SNMP использует протокол UDP, что делает его легковесным и быстрым, применимым для мониторинга большого количества устройств.

5. Активный и пассивный мониторинг: SNMP позволяет как запрашивать информацию (активный мониторинг), так и получать уведомления от устройств при возникновении определенных событий (пассивный мониторинг через TRAP-сообщения).

6. Стандартизация: как устоявшийся стандарт, SNMP обеспечивает единообразный подход к управлению сетью независимо от производителя оборудования.

7. Простота использования: базовая структура SNMP относительно проста, что облегчает его внедрение и использование.

8. Расширяемость: MIB позволяет легко добавлять новые объекты для мониторинга.

9. Безопасность в SNMPv3: последняя версия протокола предлагает надежные механизмы аутентификации и шифрования.

Минусы SNMP:

1. Ограниченная детализация данных: SNMP может не предоставлять достаточно гранулярных данных для некоторых сложных сценариев мониторинга.

2. Проблемы с безопасностью в старых версиях: SNMPv1 и SNMPv2c имеют слабый уровень защиты.

3. Ограниченная производительность: при мониторинге большого количества устройств или частых опросах SNMP может создавать значительную нагрузку на сеть.

4. Сложность настройки SNMPv3: Хотя SNMPv3 решает проблемы безопасности, его настройка может быть сложной и трудоемкой.

5. Отсутствие поддержки реального времени: SNMP не предназначен для мониторинга в реальном времени с высокой частотой обновления данных.

6. Проблемы с фаерволами: SNMP-трафик часто блокируется фаерволами, что может затруднить мониторинг через интернет или между разными сегментами сети.

Потоковая сетевая телеметрия – это механизм, использующий push модель (устройства сами отправляют данные) для непрерывной отправки данных о работе устройств с высоким разрешением в систему управления сетью. Данные отправляются с более высокой скоростью и с меньшей нагрузкой на сетевые устройства, чем другие методы, такие как pull модель в SNMP или применение инструментов с интерфейсом командной строки (CLI). Сетевые администраторы могут настраивать способ получения данных с устройств указывая периодичность отправки данных, обеспечивающую оптимальный объём информации с минимизацией нагрузки на сеть или указывают триггеры необходимых событий. Примерами триггеров событий являются превышение пороговых значений интересующих параметров, например, большое количество ошибок, или изменение интересующих состояний, например, изменение состояния сетевого интерфейса.

Преимущества потоковой телеметрии:

1. Реальное время: обеспечивает практически мгновенную видимость состояния сети, что критично для быстрого реагирования на проблемы.

2. Масштабируемость: хорошо подходит для крупных и динамичных сетевых сред с большим количеством устройств.

3. Гибкость: администраторы могут настроить, какие данные собирать и с какой частотой.

4. Поддержка аналитики больших данных: легко интегрируется с современными системами анализа и машинного обучения.

5. Эффективность использования ресурсов: несмотря на большой объём данных, часто более эффективна в использовании полосы пропускания благодаря оптимизированным протоколам.

6. Предиктивная аналитика: позволяет прогнозировать потенциальные проблемы на основе трендов и паттернов в данных.

Недостатки телеметрии:

1. Требования к оборудованию: часто требует более современного сетевого оборудования, которое поддерживает технологии потоковой телеметрии.

2. Сложность инфраструктуры: для обработки и хранения больших объёмов данных, полученных с помощью телеметрии, может потребоваться более сложная и дорогостоящая инфраструктура.

3. Кривая обучения: для эффективного использования потоковой телеметрии может потребоваться дополнительное обучение персонала.

4. Потенциальное увеличение нагрузки на сеть: при неправильной настройке может создавать значительный дополнительный трафик.

5. Проблемы безопасности: передача большого объёма детальных данных о сети может представлять риск безопасности, если не обеспечена должная защита.

6. Сложность анализа: большой объём данных может затруднить выделение действительно важной информации без применения необходимых аналитических инструментов.

Сравнение подходов в мониторинге и управлении сетью

Сетевые администраторы могут предпочесть использовать SNMP, когда им нужно получить относительно статичные данные, например, данные для инвентаризации устройств сети или данные о соседних устройствах. Однако механизм опроса SNMP затрудняет сбор больших объёмов данных о производительности с высоким разрешением.

SNMP полезен для сетей, в которых используется большое количество старых устройств, не поддерживающих новые технологии телеметрии. Он также хорош для сбора данных, например, о производительности маршрутизирующих узлов или инвентарной информации об устройствах, такой как серийные номера, модули и расположение слотов.

Наконец, использование SNMP, работающего через UDP, устраняет необходимость в выделении больших буферов приёма, что позволяет серверам управления более эффективно распределять внутреннюю память.

Сетевые администраторы могут предпочесть использовать потоковую телеметрию для сбора данных о производительности с высоким разрешением, например, статистики высокоскоростных сетевых интерфейсов. Телеметрия становится всё более практичной по мере того, как всё больше производителей устройств и систем управления сетями улучшают поддержку этой методологии.

Кроме того, новые механизмы RPC делают телеметрию более эффективной для получения данных с сетевых устройств, чем SNMP или CLI. Для некоторых сетевых администраторов телеметрия может стать очевидным выбором в будущем. Однако коллекторы телеметрических данных, использующие TCP-соединения, могут потреблять значительный объём памяти для буферов приёма, в зависимости от реализации. Более того, большое количество YANG моделей для каждого поставщика оборудования может затруднить анализ потоковых данных.

Для сетей, в которых есть как старые, так и новые сетевые устройства, лучше всего использовать комбинацию SNMP и потоковой телеметрии. Переход на телеметрию возможен, если все сетевые устройства в организации её поддерживают.

Независимо от того, как сетевые администраторы оценивают методы сбора данных телеметрии по сравнению с SNMP, управление сетью – это, по сути, проблема больших данных. Система управления должна обрабатывать большие объёмы данных, чтобы выявлять аномалии и предупреждать специалистов по эксплуатации сети о проблемах. Инициативы OpenConfig и gNMI направлены на упрощение сбора и анализа данных.

Заключение. Таким образом, можно с уверенностью сказать, что будущее сети не заключается в полном отказе от SNMP в пользу использования новых технологий, а в разумном сочетании различных подходов. SNMP, благодаря своей надежности, простоте и расширенной поддержке, останется важным компонентом в арсенале сетевых администраторов на долгие годы.

SNMP и телеметрия – это не конкуренты, а скорее партнеры в борьбе за здоровье сети. Каждый из них имеет свои сильные стороны и может быть использован для решения различных задач. Главное – правильно выбрать инструмент, который наилучшим образом соответствует потребностям вашей сети.