СОВРЕМЕННЫЕ ТЕХНОЛОГИИ

Д. С. Сильнов

АКТУАЛЬНОСТЬ СОВРЕМЕННЫХ СИСТЕМ УДАЛЕННОГО МОНИТОРИНГА ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ

Проведена классификация современных систем удаленного мониторинга вычислительных ресурсов. Обозначены текущие проблемы и перспективы их решения. Рассмотрена применимость систем в различных областях.

Ключевые слова: удаленный мониторинг, система контроля поведения, проблемы, перспективы.

D. Silnov

THE MODERN SYSTEMS OF CALCULATION RESOURCES REMOTE MONITORING

The classification of the modern systems remote monitoring. Problems and future possibilities.

Keywords: remote monitoring, antiviruses, firewalls

Предпосылки к созданию средств удаленного мониторинга появились в тот момент, когда возникла необходимость отслеживать состояние компьютерной системы, к которой нет локального доступа. Причин отсутствия доступа может быть несколько:

- территориальная удаленность системы;
- недоступность вследствие физических ограничений безопасности;
- отсутствие физических средств локального доступа.

Системы удаленного мониторинга работают по клиент-серверной модели; взаимодействие клиента и сервера осуществляется с помощью стандартных, либо же собственных протоколов, данные передаются через сети передачи данных.

Существующие системы мониторинга можно разделить на системы, реализующие активный мониторинг и пассивный (рис. 1). В данном случае под пассивным мониторингом понимается получение данных в режиме чтения. Примером таких систем могут быть те, которые собирают данные о температуре, о загрузке процессора, о потреблении оперативной памяти и прочее.

Под активным мониторингом следует понимать мониторинг с элементами воздействия на среду (операционную систему, приложения, аппаратное обеспечение). Примерами таких систем могут быть те, которые при определенных внешних условиях или же при определенных значениях параметров на компьютере выполняют корректирующее воздействие в рамках операционной системы (ОС).

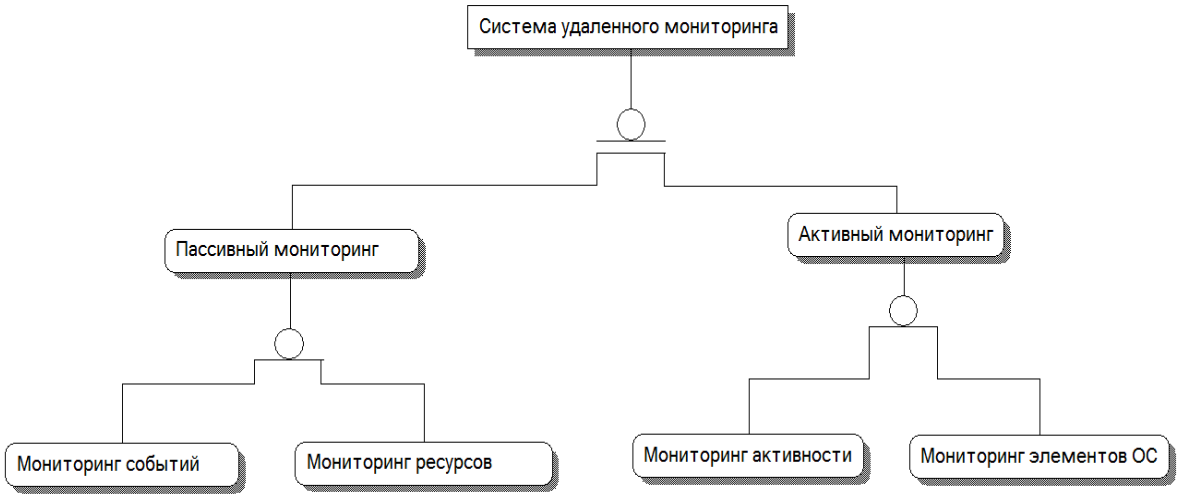

Рис. 1. Классификация систем удаленного мониторинга

Существует протокол SNMP (Simple Network Management Protocol), описанный в RFC1157 [1], работающий на прикладном уровне модели OSI, который специально был разработан для решения задач передачи данных в системах мониторинга. Передача данных осуществляется между клиентской частью системы мониторинга и серверной частью.

SNMP не определяет, какую информацию (какие переменные) управляемая система должна предоставлять. Наоборот, SNMP использует расширяемую модель, в которой доступная информация определяется базами управляющей информации MIB (Management Information Base). MIB описывают структуру управляющей информации устройств. Они используют иерархическое пространство имен, содержащее уникальный идентификатор объекта (object identifier (OID)). Каждый уникальный идентификатор объекта идентифицирует переменную, которая может быть прочитана или установлена через SNMP.

Иерархия MIB может быть изображена как дерево с безымянным корнем, уровни которого присвоены разными организациями. На самом высоком уровне MIB OID принадлежат различным организациям, занимающимся стандартизацией, в то время как на более низком уровне OID выделяются ассоциированными организациями. Эта модель обеспечивает управление на всех слоях сетевой модели OSI, так как MIB могут быть определены для любых типов данных и операций [9].

Управляемый объект — это одна из любого числа характеристик, специфических для управляемого устройства. Управляемый объект включает в себя один или более экземпляров объекта (идентифицируемых по OID), которые реально представляют собой переменные.

Существуют два типа управляемых объектов:

1. Скалярные объекты, определяющие единственный экземпляр объекта.

2. Табличные объекты, определяющие множественные, связанные экземпляры объектов, которые группируются в таблицах MIB.

Кроме SNMP существуют и собственные реализации протоколов обмена данными в системах мониторинга, но SNMP является наиболее популярным и востребованным за счет расширяемости и открытости интерфейса. Кроме этого, SNMP может быть использован как в активном мониторинге, так и в пассивном. Необходимо рассмотреть более подробно применимость как пассивного мониторинга, так и активного.

Пассивный мониторинг. Под данную классификацию попадает большинство систем мониторинга, которые используются специализированным персоналом для отслеживания возникновения неисправностей и/или нештатных ситуаций. Пассивный мониторинг предполагает сбор информации с удаленных источников в режиме чтения. Далее возможен ряд действий, среди которых — отображение данной информации оператору, а в случае изменения параметров за пределы, определенные как «нормальные», оператор принимает определенные шаги для устранения возникшей ситуации, для нормализации параметров. Формат оповещения может быть разный: это построение графиков, а также генерация сообщений в приоритетном режиме для более оперативного отображения оператору.

Мониторинг ресурсов. Одной из ключевых задач систем мониторинга является мониторинг ресурсов вычислительных устройств. Представителями подобных систем являются MRTG (Multi Router Traffic Grapher) [3] и CACTI [4]. Оба данных программных продукта являются бесплатными. Автор MRTG создал его для контроля загруженности интерфейсов на сетевых устройствах (коммутаторы и маршрутизаторы) и, как следствие, MRTG стало популярным среди компаний, работающих в области связи. Но не только загрузку каналов можно изображать в виде графиков, возможно собирать статистику с температурных датчиков (предварительно оснастив данные датчики сетевым интерфейсом, или используя специализированные устройства расширения), собирать данные о скорости вращения вентиляторов. CACTI же предлагает более удобный интерфейс, но и требует больших затрат на установку и настройку. Данные типы систем мониторинга не позволяют в режиме реального времени отслеживать какие-либо показатели, но позволяют хранить статистику и отображать ее в виде графиков. Применимость заключается, например, в том, чтобы отслеживать температуру холодильных камер и в случае возникновения проблем иметь данные об изменении температуры за сутки, за неделю, за месяц. Без участия дополнительного персонала, например, в случае отключения электроэнергии, невозможно оценить были ли размморожены камеры в период перебоя. Кроме приведенного примера отслеживания температурного режима также можно контролировать любые параметры, которые имеют критические показатели для предприятия. Это напряжение в сети, показатели давления. Рядовые сотрудники могут не заметить или умышленно скрыть превышение определенных параметров в ходе производственного процесса, что, в конечном счете, может повлиять на качество продукции. Система мониторинга — это дополнительный элемент контроля, но этот контроль не ведется в режиме реального времени.

Мониторинг событий. В связи с тем, что любая вычислительная система постоянно находится в работе и ежесекундно случаются какие-либо события как в ОС, так и на аппаратном уровне, необходимо отслеживать данные события, если они случаются в незапланированном формате. Это и срабатывание датчиков, например, превышения температуры, датчиков движения, датчиков задымленности. Для отслеживания подобных событий можно использовать такие системы мониторинга, как Nagios и Zabbix [5]. Nagios сложен в первичной настройке, но удобен при последующем использовании. Интерфейс Nagios ориентирован на наличие персонала, который следит за состоянием показателей системы. Данные поступают не в реальном времени, но время опроса элементов можно регулировать в зависимости от потребностей. Удаленные системы опрашиваются посредством программных интерфейсов [6]. Соответственно при наступлении каких-либо событий в интерфейсе выводятся соответствующие информационные сообщения. Данный программный продукт ориентирован именно на срабатывание определенных событий, в отличие от систем мониторинга ресурсов.

Активный мониторинг. Активный мониторинг характеризуется тем, что на определенные события, которые происходят, существует заранее заданное воздействие, которое

приводит предположительно к решению возникшей проблемы. То есть активный мониторинг производит воздействия, направленные на систему, в которой произошло нарушение параметров. Таким образом, активный мониторинг характерен наличием обратной связи.

Мониторинг элементов ОС. В ОС Windows в серверных версиях (Windows Server 2003, Windows Server 2008) существует стандартный механизм мониторинга работы служб (windows services). Мониторинг ориентирован на контроль работоспособности элементов служб и осуществляет определенные действия (задаваемые пользователем) в случае выхода из строя данных служб. Данный механизм применяется, например, для перезапуска сервера 1С:Предприятия версии 8 [7] в случае возникновения ошибки и разового выхода из строя. В случае, если проблема имеет разовый характер, то перезапуск позволяет продолжить работу с приложением с минимальными задержками, если же подобная система не используется, то требуется время на перезапуск данной службы вручную, а в случае, если ответственный сотрудник не находится на рабочем месте, время решения проблемы может составлять десятки минут. Это, в свою очередь, может повлечь финансовые потери из-за невозможности для бухгалтерии ведения своей деятельности.

Мониторинг активности. Мониторинг активности может быть различной активности; это и срабатывание датчиков, к примеру температуры, и увеличение оборотов вентиляторов на основании этих данных для снижения температуры. Примерами таких систем являются HP OpenView [8] и IBM Tivoli [9]. Это комплексные системы, которые можно в совокупности именовать интеллектуальными системами, генерирующие в зависимости от возникновения событий активности ответные действия для восстановления требуемых показателей. В полной же мере в эту категорию попадают системы формата «умный дом», которые активно производят мониторинг ситуации и могут совершать по заданной логике необходимые действия. Также это и комплексные системы контроля управления доступом (СКУД), которые могут принимать комплексные решения в зависимости от входных данных, например данных о сотруднике посредством RFID-пропуска.

Ключевыми современными проблемами систем удаленного мониторинга являются:

- отказ отдельных элементов или системы в целом;
- умышленное вредоносное воздействие на систему.

Отказ может быть вызван рядом причин: обрыв линий связи (в случае проводных технологий), помехи от сторонних источников сигналов (в случае беспроводных технологий). Распространенной проблемой в системах пожаротушения является обрыв датчика замкнутого контакта, когда необходимо либо отключать данный датчик для продолжения работы системы в целом, так как он вызывает срабатывание, либо же отключать систему полностью и оперативно искать обрыв. В том или ином случае подобные ошибки приводят к лишним временным тратам сотрудников, которые таким образом отвлекаются от своих непосредственных обязанностей. В случае же, когда подобные вещи происходят ночью время устранения может исчисляться часами, а в этот период система пожаротушения не работает в штатном режиме. Кроме физических причин отказа есть и программные, вызванные ошибками в ПО, а также умышленным воздействием на систему. Умышленные воздействия могут быть с целью вывода из строя системы: например, сервер видеонаблюдения может быть выведен из строя для проникновения на объект, или же данные могут умышленно искажаться. С использованием RFID-карточек (или аналогичных систем) для контроля передвижения сотрудников умышленное искажение может заключаться в желании исказить данные перемещения за счет прохода в изолированные зоны по чужим пропускам.

По мере модернизации производств, усложнения систем, увеличения доли автоматизации на смену классическому ОТК, где требуется проверять качество работы, по большей части выполненной человеком, появляется необходимость контролировать вычислительные ресурсы. Таким образом, значимость систем мониторинга будет расти. Но с ростом роли систем мониторинга необходимо уделять большее внимание вопросам правильной работы и защиты. Причем это и классические ошибки (например, отказ датчиков), которые легко диагностируются, но и умышленные воздействия для искажения результатов мониторинга или умышленный вызов отказа в обслуживании для предотвращения получения данных системой мониторинга. Таким образом, будет возрастать роль защиты систем удаленного мониторинга от внешних воздействий; системы удаленного мониторинга уже сейчас являются неотъемлемым элементом сложных систем, но часто системы мониторинга воспринимаются как побочный элемент. В данной области автором разрабатываются комплексные методы и средства защиты систем удаленного мониторинга.

СПИСОК ЛИТЕРАТУРЫ

1.1С:Предприятие 8 [Электронный ресурс] URL: http: //v8.1c.ru/ (дата обращения 05.05.2011).

2. A Simple Network Management Protocol (SNMP). URL.: http://www.ieft.org/rfc1157.txt (дата обращения: 05/05/2011).

3. IBM Tivoli — Integrated Management software [электронный ресурс] URL: http://www.ibn.com/software/tivoly (дата обращения: 05.05.2011).

4. IT Performance Suite | HP Enterprise Software [Электронный ресурс] URL: http://www.managementsoftware.hp.com (дата обращения: 05.05.2011).

5. *Josephsen David*. Building a Monitoring Infrastructure with Nagios. Prentice Hall, 2007.

6. *Lavlu Ibrahim, Kundu Dinangkur*. Cacti 0.8 Network Monitoring. Pact Publishing, 2009.

7.*Olups Rihards*. Zabbix 1.8 Network Monitoring. Packt Publishing, 2010.

8. *Shipway Steve*. Using MRTG with RRDtool and Routers2. Cheshire Cat Computing, 2010.

9. *Stallings William*. SNMP, SNMPv2, SNMPv3, and RMON 1 and 2 (3rd Edition). Addisison-Wesley Professional, 1999.

REFERENSES

1.1S:Predprijatie 8 [Elektronnyj resurs] URL: http: //v8.1s.ru/ (data obrashchenija 05.05.2011).

2. A Simple Network Management Protocol (SNMP). URL.: http://www.ieft.org/rfc1157.txt (data obrawenija: 05/05/2011).

3. IBM Tivoli — Integrated Management software [elektronnyj resurs] URL: http://www.ibn.com /software/tivoly (data obrawenija: 05.05.2011).

4. IT Performance Suite | HP Enterprise Software [Elektronnyj resurs] URL: http://www.managementsoftware.hp.com (data obrashchenija: 05.05.2011).

5. *Josephsen David*. Building a Monitoring Infrastructure with Nagios. Prentice Hall, 2007.

6. *Lavlu Ibrahim, Kundu Dinangkur*. Cacti 0.8 Network Monitoring. Pact Publishing, 2009.

7.*Olups Rihards*. Zabbix 1.8 Network Monitoring. Packt Publishing, 2010.

8. *Shipway Steve*. Using MRTG with RRDtool and Routers2. Cheshire Cat Computing, 2010.

9. *Stallings William*. SNMP, SNMPv2, SNMPv3, and RMON 1 and 2 (3rd Edition). Addisison-Wesley Professional, 1999.