Д. С. Сильнов

СОВРЕМЕННЫЕ СИСТЕМЫ УДАЛЕННОГО МОНИТОРИНГА ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ: СОСТОЯНИЕ, ПРОБЛЕМЫ, ПЕРСПЕКТИВЫ

Введение

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 собственных протоколов, данные передаются через сети передачи данных.

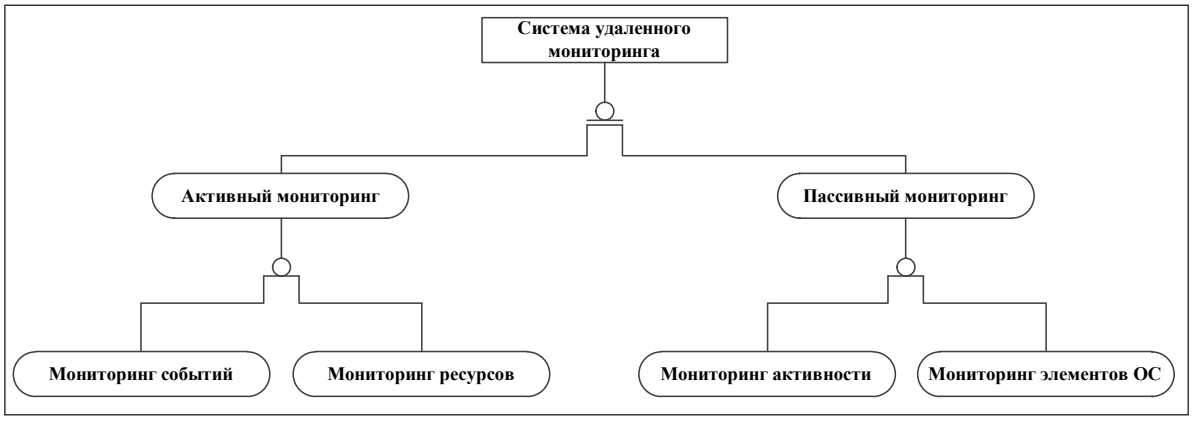

Рис. 1. Классификация систем удаленного мониторинга

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

Под активным мониторингом следует понимать мониторинг с элементами воздействия на среду (операционную систему (ОС), 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 ОС или приложения.

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 разным организациям. На самом высоком уровне MIB OID принадлежат различным организациям, занимающимся стандартизацией, в то время как на более низком уровне OID выделяются ассоциированным организациям. Эта модель обеспечивает управление на всех слоях сетевой модели OSI, так как MIB могут быть определены для любых типов данных и операций [2].

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.

Существует два типа управляемых объектов:

1. Скалярные объекты определяют единственный экземпляр объекта;

2. Табличные объекты определяют 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. Помимо этого, SNMP может быть использован как при активном, так и при пассивном мониторинге.

Пассивный мониторинг. В данный класс 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, например отображение информации перед оператором. В случае выходов значений параметров за пределы, определенные как «нормальные», оператор предпринимает соответствующие шаги для устранения возникшей ситуации в целях нормализации параметров. Формат оповещений может быть разным, это и построение графиков, а также генерация сообщений в приоритетном режиме для более своевременного отображения данных для оператора.

Мониторинг ресурсов. Одна из ключевых задач систем мониторинга — мониторинг ресурсов вычислительных устройств. Представителями подобных систем являются MRTG (Multi Router Traffic Grapher) [3] и CACTI [4]; оба программных продукта являются бесплатными, с открытым кодом. 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, сведения о скорости вращения вентиляторов и т. п. (предварительно оснастив соответствующие датчики сетевым интерфейсом или используя специализированные устройства расширения). CACTI же предлагает более удобный интерфейс, но требует больших затрат на установку и настройку. Данные типы систем мониторинга не позволяют в режиме реального времени отслеживать какие-либо показатели, но имеют возможность хранить статистику и отображать ее в виде графиков. Применимость заключается, например, в том, чтобы отслеживать температуру холодильных камер, а в случае возникновения проблем иметь данные об изменении температуры за сутки, неделю, месяц и т. д. Это позволит без участия дополнительного персонала, например, в случае отключения электроэнергии оценить, были ли размерожены камеры в период перебоя. Кроме приведенного примера отслеживания температурного режима можно контролировать любые другие параметры, которые имеют критическое значение для предприятия. Это напряжение в сети, показатели давления, уровень шума, концентрация вредных веществ и т. п. Рядовые сотрудники могут не

заметить либо умышленно скрыть превышение определенных пороговых параметров в ходе производственного процесса, что, в конечном счете, может повлиять на качество продукции.

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. Например, это превышение температуры, срабатывание 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 режиме реального 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 при наступлении 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 предположительно приводит к решению возникшей проблемы. Т. е. при активном мониторинге производятся 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. Этот механизм применяется, например, для перезапуска сервера 1С:Предприятия версии 8 [7] в случае возникновения ошибки и разового выхода из строя. Когда проблема имеет разовый характер, 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 природы, к примеру, это срабатывание датчиков 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, как правило, требуют значительных финансовых затрат на их внедрение. Подобные продукты обычно представляют собой интеллектуальные системы, которые в зависимости от возникновения событий активности генерируют ответные действия для восстановления требуемых показателей. В полной мере в эту категорию попадают системы «умных домов», которые активно производят мониторинг ситуации и могут совершать по заданной логике необходимые действия. Также сюда можно отнести и комплексные системы контроля управления доступом (СКУД), которые могут принимать сложные решения в зависимости от входных данных, например сведений о сотруднике посредством RFID-пропуска.

Ключевыми *проблемами* систем удаленного мониторинга являются:

- отказы и/или сбои отдельных элементов или системы в целом;
- умышленное вредоносное воздействие на систему.

Отказ или сбой (перемежающийся или самоустранимый 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 отказ датчика типа 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 затратам сотрудников, которые таким образом отвлекаются от своих непосредственных обязанностей. Если же подобные вещи происходят ночью, то время устранения может исчисляться часами, причем в этот период система пожаротушения не будет работать в штатном режиме и при возникновении реального пожара он не будет своевременно обнаружен. Кроме физических причин отказа есть и программные, вызванные ошибками в ПО, а также умышленным воздействием на систему. Умышленные воздействия могут предприниматься 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 данных о перемещении может иметь целью проход в изолированные зоны по чужим пропускам.

Заключение

По мере модернизации производств, усложнения систем, увеличения доли автоматизации на смену классическому ОТК (отдел технического контроля), где требуется проверять качество работы сотрудников, приходит необходимость контролировать вычислительные ресурсы. Таким образом, значимость систем мониторинга будет расти. Но с ростом роли систем мониторинга придется уделять все большее внимание вопросам их правильной работы и защиты.

Кроме того, системы удаленного мониторинга зачастую воспринимаются штатными системами обеспечения безопасности (антивирусы, брандмауэры и др.) как вредоносные, поскольку они могут генерировать значительный объем трафика, напрямую обращаться к аппаратным ресурсам. В итоге работоспособность систем удаленного мониторинга также будет нарушена.

Учитывая все вышесказанное, в обозримом будущем необходимость защиты систем удаленного мониторинга от внешних воздействий будет постоянно возрастать, а значит, разработка средств защиты систем удаленного мониторинга будет актуальной научно-практической задачей.

СПИСОК ЛИТЕРАТУРЫ:

1. *Case J., Fedor M., Schoffstall M., Davin J.* Request for Comments: 1157. [Электронный ресурс] URL: http://www.ietf.org/rfc/rfc1157.txt (дата обращения: 08.08.2011).
2. *Stallings W.* SNMP, SNMPv2, SNMPv3, and RMON 1 and 2. 3rd Edition. Toronto, CA: Addison-Wesley Professional, 1999.
3. *Shipway S.* Using MRTG with RRDtool and Routers2. Cheshire Cat Computing publication, 2010.
4. *Lavlu S. M. I., Kundu D.* Cacti 0.8 Network Monitoring. Birmingham, UK: Packt Publishing Ltd., 2009.
5. *Olups R.* Zabbix 1.8 Network Monitoring. Birmingham, UK: Packt Publishing Ltd., 2010.
6. *Josephsen D.* Building a Monitoring Infrastructure with Nagios. Boston, USA: Prentice Hall, 2007.
7. http://v8.1c.ru.
8. http://www.managementsoftware.hp.com.
9. www.ibm.com/software/tivoli/.