УДК 004.72

Э.М. Мехтиев, В.П. Комагоров, О.Б. Фофанов, А.В. Марчуков

К вопросу о проектировании системы мониторинга корпоративной вычислительной сети

Рассматриваются вопросы проектирования архитектуры системы мониторинга корпоративной вычислительной сети, включающей в себя подсистему мониторинга сетевой инфраструктуры и подсистему мониторинга информационных систем различного назначения. Определены функциональные требования, которым должна удовлетворять система мониторинга в целом. Изложен метод оценки эффективности пакетов программ при их выборе для построения каждой из подсистем. Предложены программные продукты для построения единой комплексной системы мониторинга.

Ключевые слова: система мониторинга, вычислительная сеть, сетевая инфраструктура, информационная система, пакет программ.

Для обеспечения надежного функционирования корпоративной вычислительной сети необходимо создание единой комплексной системы мониторинга [1, 2], включающей в себя две составные части: подсистему мониторинга сетевой инфраструктуры и подсистему мониторинга информационных систем различного назначения.

В состав сетевой инфраструктуры входят коммуникационное и серверное оборудование, а также каналы передачи данных: кабельные, радиорелейные (РРЛ), системы спутниковой связи (ССС). Подсистема мониторинга сетевой инфраструктуры предназначена для оперативного контроля состояния ее основных компонент с целью обнаружения блокировок и узких мест при передаче данных и их последующего устранения.

Эффективность функционирования информационных систем определяется не только производительностью самого сервера, но и составом и характеристиками сетевых приложений. Основным назначением подсистемы мониторинга информационных систем является оперативный контроль функционирования сетевых приложений с целью выявления приложений, блокирующих или монополизирующих каналы передачи данных, и организация их работы таким образом, чтобы обеспечить требуемое качество обслуживания абонентов сети.

Единая комплексная система мониторинга корпоративной вычислительной сети должна отвечать следующим функциональным требованиям:

• в основу построения системы мониторинга корпоративной вычислительной сети должны быть положены стандартизированные технологии, использующие протокол SNMP [3];

• представление корпоративной вычислительной сети в виде интерактивной схемы, отображающей работоспособность каналов передачи данных, коммутаторов, маршрутизаторов, объемы передаваемой информации, места блокировок в сети;

• возможность корректировки интерактивной схемы при развитии вычислительной сети (появление новых каналов передачи данных, коммуникационного и серверного оборудования, сетевых абонентов);

• сбор и хранение в базе данных информации о работоспособности каналов передачи данных, коммуникационного и серверного оборудования, величине и характере сетевого трафика, распределении трафика по сетевым абонентам и приложениям;

• удаленный доступ к базе данных системы мониторинга на основе технологий Web-клиент с проверкой пароля и прав доступа к запрашиваемой категории информации;

• получение сводных отчетов о наиболее и наименее загруженных сегментах сети, работе сетевых приложений и качестве обслуживания абонентов;

• фоновый режим работы системы мониторинга, исключающий блокировки в сети при сборе диагностической информации в реальном масштабе времени и ее загрузке в базу данных.

В данной статье рассматриваются вопросы проектирования архитектуры системы мониторинга корпоративной вычислительной сети, включающей в себя подсистему мониторинга сетевой инфраструктуры и подсистему мониторинга информационных систем различного назначения. Она содер-

жит описание методов анализа и оценки эффективности типовых пакетов программ при их выборе для построения каждой из подсистем. При этом выбранные пакеты программ должны в значительной степени обеспечивать возможность построения единой комплексной системы мониторинга, отвечающей перечисленным ранее функциональным требованиям. В заключении предложены программные системы для построения единой комплексной системы мониторинга.

Исходным материалом для данной статьи явились результаты выполнения 1-го этапа договора Института кибернетики Томского политехнического университета и ОАО «Томскнефть» ВНК на тему «Создание прототипа системы мониторинга сетевой инфраструктуры и информационных систем ОАО «Томскнефть» ВНК». Следует отметить, что изложенный в статье подход к проектированию системы мониторинга корпоративной вычислительной сети может быть использован другими предприятиями и организациями, имеющими развитую вычислительную сеть.

Оценка эффективности и выбор пакетов программ для построения подсистемы мониторинга сетевой инфраструктуры. Выбор пакетов программ для мониторинга состояния компьютерного и каналообразующего оборудования, систем и средств связи является ключевым моментом при проектировании прототипа будущей разрабатываемой подсистемы, которая позволила бы оптимизировать процесс принятия решений при возникновении проблемных ситуаций как на отдельных участках сетевой инфраструктуры, так и сети в целом.

Для оценки эффективности пакетов программ, которые могут быть использованы при построении подсистемы мониторинга инфраструктуры сети, представляется целесообразным выполнить следующие действия:

- определить перечень основных функций подсистемы;
- присвоить каждой функции значение ранга, определяющего ее значимость для мониторинга инфраструктуры сети;
- выполнить анализ пакетов программ на соответствие перечню функций подсистемы;
- рассчитать суммарное значение ранга для каждого из анализируемых пакетов.

Некоторые функции подсистемы мониторинга и значения их рангов, установленных экспертами, в качестве которых выступали сетевые администраторы, приведены в таблице.

Состав основных функций подсистемы мониторинга сетевой инфраструктуры и значения их рангов

№ п/п	Функция	Описание	Ранг
1	События	Отображение всех типов событий, происходящих в сети	10
2	Прогнозирование событий	Наличие алгоритмов для прогнозирования событий и формирования статистики	5
4	SNMP	Поддержка SNMP-агента	8
•	• • • •	• • • •	•
19	Наличие карты или схемы сети	Функция визуального отображения текущего состояния узлов на карте	9
20	Автоматическое формирование отчетов	Возможность автоматической выгрузки отчетов в различных форматах	12
21	Доступ через Web-интерфейс	Наличие функции доступа через Web-интерфейс к пакету программ	8
	Итого		100

Вычисление суммарного ранга пакета программ, который может быть использован при построении подсистемы мониторинга сетевой инфраструктуры, осуществляется по следующему выражению:

$$R_i = \sum_{j=1}^{m} V_j * L_{ij},$$

где R_i – суммарный ранг i-го пакета программ, принимающий значения от 0 до 100 (i изменяется от 1 до n, где n – количество анализируемых пакетов программ); V_j – ранг j-й функции (j изменяется от 1 до m, где m – количество функций подсистемы мониторинга); L_{ij} – вес j-й функции i-го пакета программ, принимает значения 1 («Да» − функция присутствует) или 0 («Нет» – функция отсутствует).

При проектировании подсистемы мониторинга сетевой инфраструктуры был проведен анализ известных типовых пакетов программ (n = 28). При этом учитывалась полнота выполняемых пакетами функций мониторинга (m = 21), определяемая значениями их суммарных рангов. Наибольшее значение ранга получил пакет программ SolarWinds NPM (R_i = 97) [4, 5]. Вместе с тем можно рекомендовать к применению и другие коммерческие программные продукты: ManageEngine OpManager (R_i = 95), HP Network node Manager (R_i = 94), Cisco LMS (R_i = 87). Данные программные продукты более всего подходят для мониторинга корпоративных сетей, насчитывающих более 5000 устройств, и гарантируют стабильную работу при больших нагрузках. В этих пакетах также реализована функция плановой выгрузки отчетов в различных форматах (txt, excel, csv).

При незначительном количестве устройств (несколько сотен) можно воспользоваться бесплатными пакетами программ, такими как Pandora FMS (R_i = 87), Icinga (R_i = 83), Nagios (R_i = 83), Open NMS (R_i = 83), Zabbix (R_i = 83), которые рассчитаны на малые и средние предприятия, однако нуждаются в значительных затратах на доработку, сопровождение и настройку под конкретные задачи предприятия.

Оценка эффективности и выбор пакетов программ для построения подсистемы мониторинга информационных систем. Подсистема мониторинга информационных систем предназначена для оперативного контроля работы серверов, сетевых приложений и сервисов, оценки эффективности их функционирования, выявления приложений, блокирующих или монополизирующих каналы передачи данных, и автоматического формирования сводных отчетов о качестве обслуживания сетевых абонентов.

При проектировании подсистемы мониторинга информационных систем проводился анализ 3 часто используемых для решения перечисленных задач пакетов программ: SolarWinds Server & Application Monitor, Microsoft System Center Operations Manager, HP Open View Smart Plug In.

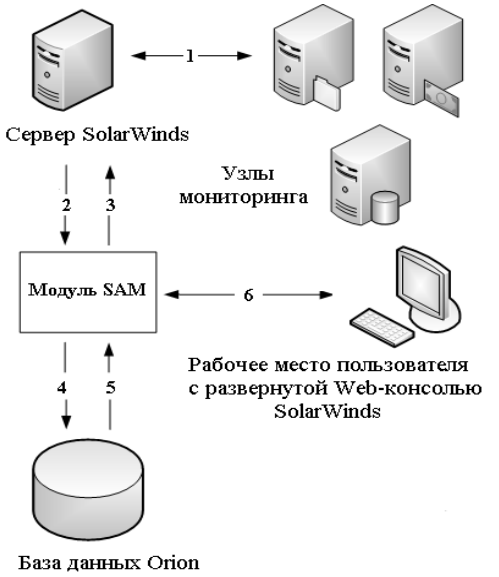

Рис. 1. Схема работы SolarWinds SAM как компонента комплексного решения SolarWinds Orion

Пакет программ SolarWinds Server & Application Monitor (SolarWinds SAM) [6] позволяет создавать и контролировать наборы данных о состоянии таких компонентов сети, как серверное оборудование и сетевые приложения. При этом SolarWinds SAM может функционировать как самостоятельно, так и в качестве компонента комплексного решения SolarWinds Orion. Структурная схема работы SolarWinds SAM как компонента комплексного решения SolarWinds Orion приведена на рис. 1.

На схеме работы SolarWinds SAM (см. рис. 1) стрелками обозначены следующие направления информационных потоков: *1* − запрос данных о приложениях и серверах на основе шаблонов и мониторов компонент; *2* − запросы по расписанию; *3* − возвращаемая статистика; *4* − запись статистики мониторинга в базу данных; *5* − возвращение запрошенных модулем SolarWinds SAM данных; *6* − отображение статистики работы приложений, времени отклика и текущего состояния.

Вместе с тем SolarWinds SAM обладает рядом особенностей, которые снижают эффективность его применения в качестве полноценного решения при формировании аналитической отчетности. К их числу относятся: отсутствие возможности ввести дополнительную классификацию приложений, необходимую администратору сети для определения их местоположения; необходимость обращения к инструментам администратора сети для создания параметризованных запросов к статистическим данным; невозможность отслеживания пороговых значений допустимого количества сбоев ответственными за эксплуатацию сети и приложений и т.д.

Пакет программ Microsoft System Center Operations Manager (MS SCOM) [7] предназначен для мониторинга сетевых устройств, поддерживающих SNMP. Он позволяет выполнять максимальный

контроль практически всех серверных продуктов и технологий Microsoft, таких как Windows Server, SQL Server, Exchange. Кроме того, MS SCOM осуществляет поддержку и мониторинг систем на базе UNIX, Linux, СУБД MySQL и Oracle.

В соответствии с перечисленными функциями MS SCOM может быть использован для построения подсистемы мониторинга серверов и приложений, а также формирования статистических отчетностей. Однако необходимо учитывать некоторые особенности его применения. В первую очередь это высокие требования к программной инфраструктуре, так как наибольшей эффективности от применения MS SCOM можно добиться только в случае наличия развернутых контроллера домена и служб DNS (является обязательным требованием при установке MS SCOM). Такие же требования предъявляются и к аппаратным средствам: для обеспечения надежной работы MS SCOM сервера сбора данных должны располагаться на отдельных выделенных физических машинах. Кроме того, MS SCOM не является комплексным решением мониторинга сетевой инфраструктуры: для формирования четкого ответа на вопрос, на каком уровне произошел сбой (сеть или приложение), необходимо наличие дополнительных вспомогательных средств мониторинга устройств сети.

Пакет программ HP Open View Smart Plug In [8] предназначен для мониторинга серверов и сетевых приложений. Он позволяет осуществлять: мониторинг аппаратных сбоев и сбоев в операционных системах; мониторинг производительности серверов, приложений и сетевых сервисов; мониторинг состояния бизнес-процессов с предоставлением информации мониторинга в единой WEB-консоли. Агенты HP Operations Manager могут устанавливаться на управляемые системы, доступны для различных платформ (UNIX, Linux, Windows) и обеспечивают сбор, агрегирование и корреляцию необходимой для мониторинга информации.

Вместе с тем применение пакета программ HP Open View Smart Plug In ограничено высокими требованиями к характеристикам серверов приложений; сложностью сопровождения, требующего наличия специалистов, умеющих работать с этим пакетом; и высокой стоимостью лицензий.

Заключение. Результаты анализа и выбора существующих программных продуктов свидетельствуют о том, что для построения подсистемы мониторинга сетевой инфраструктуры целесообразно использовать пакет программ Solarwinds NPM, а для построения подсистемы мониторинга информационных систем могут быть применены три пакета программ: SolarWinds SAM, MS SCOM и HP Open View Smart Plug In, каждый из которых имеет свои преимущества и недостатки.

Система мониторинга корпоративной вычислительной сети представляет собой единый комплекс технических и программных средств, обеспечивающий контроль работы компьютерного и каналообразующего оборудования, систем и средств связи, сетевых приложений и сервисов с целью оценки эффективности их функционирования и автоматического формирования сводных отчетов о качестве обслуживания сетевых абонентов.

В связи с этим представляется целесообразным осуществить построение единой комплексной системы мониторинга на основе пакетов программ Solarwinds NPM и SolarWinds SAM, являющихся составными частями программного продукта Solarwinds Orion. Такое решение обеспечит надежное функционирование системы мониторинга [9] в рамках единого информационного пространства.

Литература

1. Общие сведения о мониторинге и измерении процессов. Принципы мониторинга. Методы мониторинга [Электронный ресурс]. – Режим доступа: http://be5.biz/ekonomika/mkms/84.htm, свободный (дата обращения: 16.05.2012).

2. Мониторинг работы Java-приложений. – Ч. 1. Мониторинг производительности и степени готовности Java-систем [Электронный ресурс]. – Режим доступа: http://www.ibm.com/developerworks/ru/library/j-rtm1, свободный (дата обращения: 16.05.2012).

3. Протокол управления SNMP [Электронный ресурс]. – Режим доступа: http://book.itep.ru/4/44/snm_4413.htm, свободный (дата обращения: 16.05.2012).

4. Orion NPM Datasheet [Электронный ресурс]. – Режим доступа: http://www.solarwinds.com/resources/datasheets/SolarWinds_OrionNPM_Datasheet.pdf, свободный (дата обращения: 16.05.2012).

5. Orion Network Performance Monitor [Электронный ресурс]. – Режим доступа: http://www.solarwinds.com/products/network-management/network-performance-monitor.aspx, свободный (дата обращения: 16.05.2012).

6. SolarWinds Server & Application Monitor Administrator Guide [Электронный ресурс]. – Режим доступа: http://inreachsolutions.com/guides/SAM_Admin_Guide.pdf, свободный (дата обращения: 16.05.2012).

7. System Center Operations Manager 2007 [Электронный ресурс]. – Режим доступа: http://technet.microsoft.com/ru-ru/library/bb310604, свободный (дата обращения: 16.05.2012).

8. Программное обеспечение HP Operations Manager [Электронный ресурс]. – Режим доступа: http://www8.hp.com/ru/ru/software/software-product.html?compURI=tcm:172-936955, свободный (дата обращения: 16.05.2012).

9. Мещеряков Р.В. Модели надежности передачи информации в защищенной распределенной телекоммуникационной сети / Р.В. Мещеряков, А.Ю. Крайнов, А.А. Шелупанов // Изв. Том. политех. ун-та. – 2008. – Т. 313, № 5. – С. 60–63.

Мехтиев Эльчин Мехтиевич
Начальник службы ИКТ ОАО «Томскнефть» ВНК
Тел.: 8-913-806-52-25
Эл. почта: MehtievEM@tomskneft.ru

Комагоров Владимир Петрович
Канд. техн. наук, доцент каф. оптимизации систем управления Национального исследовательского Томского политехнического университета (НИТПУ)
Тел.: 8-913-106-20-10
Эл. почта: komagorov@tpu.ru

Фофанов Олег Борисович
Канд. техн. наук, зав. каф. оптимизации систем управления НИТПУ
Тел.: 8-913-848-17-55
Эл. почта: ofofano@tpu.ru

Марчуков Артур Викторович
Зав. лабораторией сетей ЭВМ и телекоммуникаций НИТПУ
Тел.: 8-913-885-84-90
Эл. почта: orion@cc.tpu.edu.ru

Mekhtiev E.M., Komagorov V.P., Fofanov O.B., Marchukov A.V.

On the issue of designing a monitoring system for corporate network

The article addressed issues of designing a monitoring system architecture for a corporate network. The systems include solutions for monitoring network infrastructure and information systems of different purposes. In the proposed approach the functional requirements of the monitoring systems are defined; efficiency assessment methodology applied to software packages for each solution is described; software products for a single monitoring system are proposed.

Keywords: monitoring system, corporate network, network infrastructure, software package.
