УДК 681.3(075)

Г.Д. Киселев, канд. техн. наук, М.С. Шпакаускас

Мониторинг мультисервисных компьютерных сетей средствами системы Nagios

Рассматривается подход к обеспечению надежности и эффективности мультисервисной компьютерной сети учебного подразделения ВУЗа с помощью применения средств мониторинга.

Approach to providing of multiservice computer network reliability and efficiency of University educational department is examined by application of monitoring facilities.

Введение

Компьютерная сеть учебной кафедры ВУЗа- в некотором смысле живой, быстро развивающийся организм, все компоненты которого неразрывно связаны. Логика развития компъютерных сетей и сетей учебных заведений, в частности, приводит к сближению комп. Содаются так называемые мультисервисные сети, предоставляющие услуги как компьютерных, так и телекоммуникационных сетей. Мультисервисная сеть – комплекс программно-аппаратных средств для предоставления услуг именуемых сервисами, которые включают средства захвата, обработки, хранения, учета и передачи через сеть пользователю вычислительной ынформации, аудио– и видео–информации с целью ее круглосуточной обработки. Возрастание сложности сетей усложняет процесс администрирования, который включает задачи устранения неисправностей аппаратной части, установки новых служб и протоколов, настройки программного обеспечения и, наконец, поиск путей оптимизации работы сети. Очень важной задачей при администрировании сетей больших масштабов является своевременное реагирование на возникающие проблемы и их устранение в минимально возможные сроки. Для оперативного и эфективного решения задач администрирования необходима достоверная информация о работе компонентов и систем сети. Эта информация может быть собрана и обработана, в частности, с помощью специальных программных систем мониторинга. Необходим инструмент, который позволит из одной точки получить полную картину функционирования всей сети.

Выбор способов и объектов мониторинга сети зависит от множества факторов – размера ИТ-инфраструктуры кафедры, конфигурации сети, используемого в ней оборудования, действующих сервисов и служб, а также конфигурации серверов и установленного на них программного обеспечения, возможностей программного обеспечения, используемого для мониторинга и т.п. Правильный выбор системы мониторинга, это гарантия стабильной и успешной работы всей инфраструктуры сети учебного подразделения.

Использование систем мониторинга и управления ИТ-инфраструктурой позволяет:

- проверить физическую доступность оборудования и оптимизировать использование информационных ресурсов;
- повысить качество ИТ-сервисов и скорость устранения сбоев в работе оборудования и программного обеспечения;
- обеспечить надежность, безопасность и согласованное функционирование всех компонентов ИТ-инфраструктуры;
- облегчить модернизацию ИТ-инфраструктуры;
- в несколько раз повысить эффективность работы системных администраторов.

Начальный этап любой проверки – тестирование физической доступности оборудования (которая может быть нарушена в результате отключения самого оборудования либо отказе каналов связи). Как минимум, это означает проверку доступности по ICMP-протоколу (ping), причем желательно проверять не только факт наличия ответа, но и время прохождения сигнала, и количество потерянных запросов: аномальные значения этих величин, как правило, сигнализируют о серьезных проблемах в конфигурации сети. Некоторые из этих проблем легко отследить при помощи трассировки маршрута (traceroute) – ее также можно автоматизировать при наличии «эталонных маршрутов».

Следующий этап – проверка принципиальной работоспособности критичных служб. Как правило, это означает TCP-подключение к соответствующему порту сервера, на котором должна быть запущена служба, и, возможно, выполнение тестового запроса (например, аутентификации на почтовом сервере по протоколу SMTP или POP или запрос тестовой страницы от веб-сервера). В большинстве случаев, желательно проверять не только факт ответа службы/сервиса, но и задержки – впрочем, то

относится уже к следующей по важности задаче: проверке нагрузки. Помимо времени отклика устройств и служб для различных типов серверов существуют другие принципиально важные проверки: память и загруженность процессора (веб-сервер, сервер БД), место на диске (файл-сервер), и более специфические – например, статус принтеров у сервера печати.

Развернутый сравнительный анализ наиболее популярных современных средств мониторинга приводится в работе [1]. Самая, возможно, известная и наиболее часто применяемая программа для мониторинга называется Nagios [2, 3]. Пакет с открытым исходным кодом предназначен для получения наглядного представления о состоянии сети, в том числе и в крупных инсталляциях. Программное обеспечение состоит из демонов и подключаемых модулей мониторинга и по своему функциональному охвату может соперничать с коммерческими продуктами. Nagios широко применяется в средах высокопроизводительных вычислений и не только в них. Сравнить параметры Nagios с параметрами некоторых аналогичных систем мониторинга можно в таблице 1.

Таблица 1. Оценка основных параметров Nagios

	Nagios	**Cacti**	**OpenNMS**	**AggreGate Network Manager**	**Zabbix**
Диаграммы	Да	Да	Да	Да	Да
Логическое группирование	Да	Нет	Нет	Да	Да
Trend Prediction (прогнозирование событий)	Нет	Неизвестно	Неизвестно	Нет	Неизвестно
Автоматический Discovery	Через плагин	Через плагин	Да	Да	Да
SNMP	Через плагин	Да	Да	Да	Да
Syslog	Через плагин	Нет	Нет	Да	Да
Внешние скрипты	Да	Да	Да	Да	Да
Плагины	Да	Да	Да	Да	Да
Уровень создания плагинов	Лёгкий	Средний	Неизвестно	Средний	Лёгкий
Триггеры/Тревоги	Да	Да	Да	Да	Да
Доступ через Web	Просмотр, Отчёты, Управление	Полный доступ	Полный доступ	Полный доступ	Полный доступ
Инвентаризация	Через плагин	Нет	Да (ограничено)	Нет	Да
Метод хранения данных	Плоская база данных, SSQLQL	RRDtool, MySQL, PostgreSQL	RRDtool, PostgreSQL	SQL	SQLite, MySQL, PostgreSQL, Oracle
Лицензия	GNU GPL	GNU GPL	GNU GPL	Коммерческая	GNU GPL
Карты	Динамические и настраиваемые	Через плагин (Weathermap)	Да	Да	Да
Управление доступом	Да	Неизвестно	Неизвестно	Да	Да
События	Да	Неизвестно	Да	Да	Да
Язык	C	PHP (requirements)	Java	Java	C - агент, сервер, прокси; PHP -фронтенд

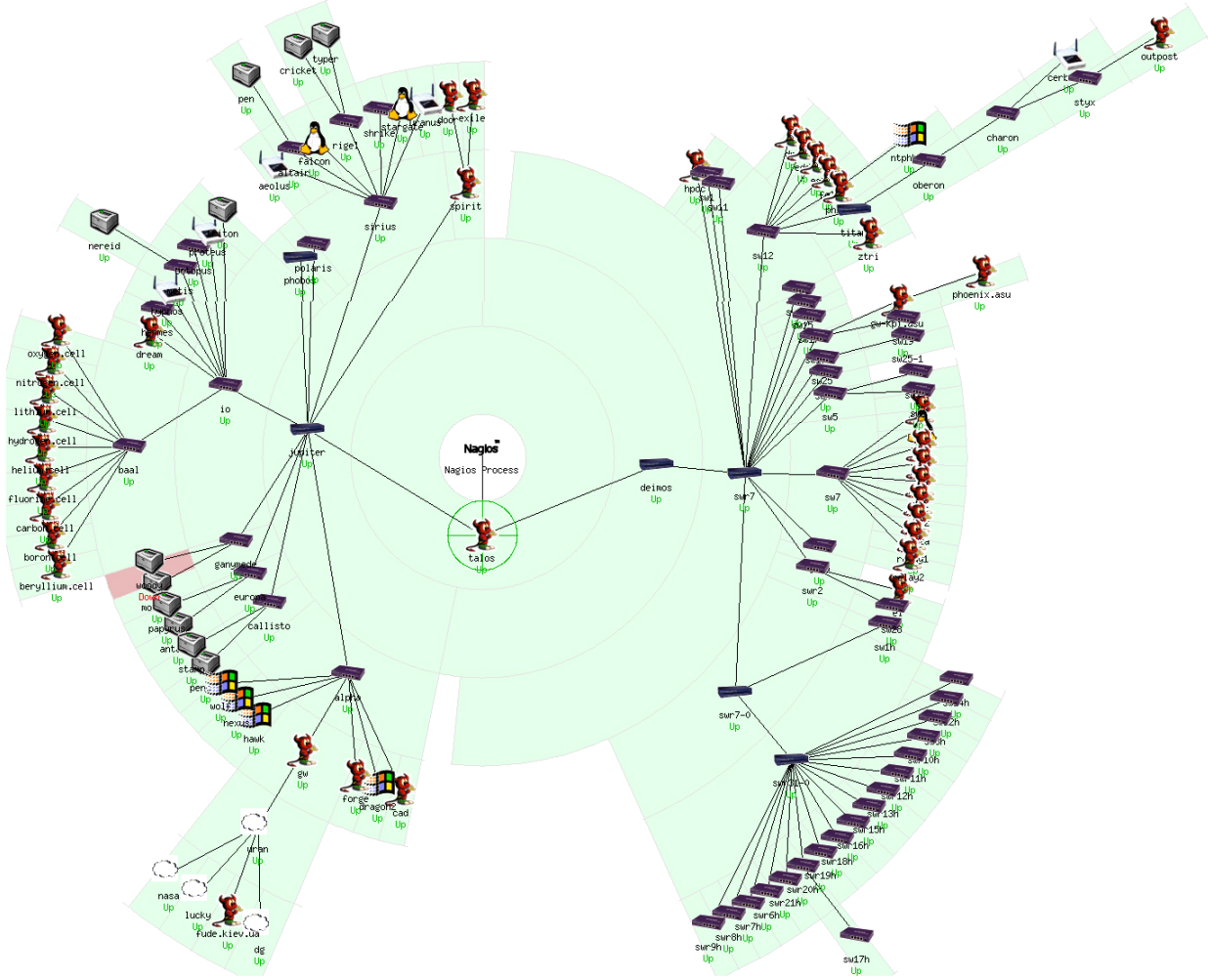

Рис. 1. Пример карты компьютерной сети построенной системой мониторинга Nagios

Обзор основных возможностей:

- Мониторинг сетевых служб (SMTP, POP3, HTTP, NNTP, ICMP, SNMP)
- Мониторинг состояния хостов (загрузка процессора, использование диска, системные логи). В большинстве сетевых операционных систем, даже Microsoft Windows с модулем NRPE_NT
- Поддержка удаленного мониторинга через шифрованные туннели SSH или SSL
- Простая архитектура модулей расширений (плагинов) позволяет, используя любой язык программирования по выбору (Shell, C++, Perl, Python, PHP, C# и другие), легко разрабатывать свои собственные способы проверки служб
- Параллельная проверка служб
- Возможность определять иерархии хостов сети с помощью «родительских» хостов, позволяет обнаруживать и различать хосты, которые вышли из строя, и те, которые недоступны
- Отправка оповещений в случае возникновения проблем со службой или хостом (с помощью почты, пейджера, смс, или любым другим способом, определенным пользователем через модуль системы)
- Возможность определять обработчики событий произошедших со службами или хостами для проактивного разрешения проблем
- Автоматическая ротация лог-файлов
- Возможность организации совместной работы нескольких систем мониторинга с целью повышения надёжности.

Для работы Nagios'a необходим сервер с установленной на нем операционной системой Linux или UNIX, web-сервером и библиотекой gd [3, 4]. Web-сервер необходим только для Web-интерфейса системы мониторинга и может не устанавливаться. Возможна установка в конфигурации с резервированием. Для мониторинга серверов используются протоколы SNMP, WMI или устанавливаются отдельные приложения NRPE или NCSA. Кроме того, возможно использовать внешнюю базу данных для хранения мониторинговой информации (MySQL). Конфигурация системы мониторинга Nagios осуществляется посредством конфигурационных файлов, где производится описание мониторящихся систем и сервисов, зависимости между ними, интервалов проверок, настройка реакций на происходящие события и оповещений [5, 6].

После того как будут сконфигурированы хосты и службы для мониторинга, можно приступать собственно к процессу запуска Nagios.
На сегодняшний день установка и конфигурирование Nagios не составляет большой проблемы, так как в сети Интернет есть масса русскоязычной документации по установке и настройке данного приложения.

Применение

Система мониторинга на основе Nagios была внедрена и используется на кафедре системного проектирования ННК «ИПСА» НТУУ «КПИ». Основными требованиями к инсталяции было построить систему, которая сможет мониторить всю кафедральную сеть и сетевые сервисы для своевременного оповещения системных администраторов о возникающих аварийных ситуациях.

Применение системы мониторинга позволило обеспечить требуемые надежность, безопасность и согласованное функционирование всех компонентов сети кафедры, повысить качество предоставляемых сервисов, устранить сбои в работе оборудования и программного обеспечения, оптимизировать использование информационных ресурсов кафедры, а так же в несколько раз повысить эффективность работы пользователей компьютерной сети.

На данный момент мониторится более ста устройств, включая сервера, коммутаторы, принтеры и т.д. В случае сбоя в работе оборудования или программного обеспечения системные администраторы оповещаются посредством электронной почты или с помощью сообщений, отправляемых на мобильный телефон. Такое своевременное оповещение позволяет максимально сократить простои оборудования и время отсутствия предоставляемых сервисов. Пример карты информационной сети кафедры, построенной системой Nagios приведен на рисунке1.

Выводы

Мультисервисные сети в большинстве своём создаются для организаций, где оборудование, операционные системы, технологии не однородны, что особенно актуально для компьютерной сети подразделения ВУЗа. Как правило, подобные сети требуют круглосуточного наблюдения, особенно если они являются частью большой ИТ-инфраструктуры. Любая компьютерная сеть, даже небольшая, требует постоянного внимания к себе. Как бы хорошо она ни была настроена, насколько бы надежное ПО не было установлено на серверах и клиентских компьютерах – нельзя полагаться лишь на внимание системного администратора; необходимы автоматические и непрерывно действующие средства контроля состояния сети и своевременного оповещения о возможных проблемах. Выбор системы Nagios для мониторинга мультисервисной компьютерной сети кафедры технического университета, ведущей подготовку специалистов по компьютерным наукам себя полностью оправдал и позволил строить технически обоснованные прогнозы развития сети.

Литература

1. *Сюзанна Франке*. Сеть на прицеле – http://www.osp.ru/lan/2005/03/140288/_p2.html
2. *Nagios* Wiki http://wiki.nagios.org/index.php/Main_Page
3. Comprehensive IT Infrastructure Monitoring – http://nagios.org/
4. *Осваиваем* Nagios – http://onix.opennet.ru/content/view/20/26/
5. *Обеспечение* работы системы мониторинга Nagios – http://www.opennet.ru/tips/info/1791.shtml
6. *Nagios* конфигурирование– http://www.berghowto.info/viewtopic.php?f=67&t=298