УДК 004.725, 004.418.

МОНИТОРИНГ И УПРАВЛЕНИЕ СЕТЬЮ ПЕРЕДАЧИ ДАННЫХ

Дрейман И. А., Капуста А. П.,
научный руководитель канд. техн. наук Кузнецов А. С.
Сибирский федеральный университет
Институт космических и информационных технологий

У многих современных предприятий имеются локальные сети, в состав которых входят: серверы, точки доступа, персональные рабочие станции и прочее сетевое оборудование, выполняющее вспомогательные, и одновременно, очень важные функции. Как правило, локальная сеть предприятий имеет одну или более точек выхода во внешние глобальные сети, в том числе в Интернет.

Большинство компаний и предприятий, постоянно развивают свою сетевую инфраструктуру, добавляя новые сервера и сетевое оборудование для создания дополнительных информационных ресурсов.

С каждым днем появляются более новые, высокопроизводительные технические решения, которые позволяют увеличить эффективность инфраструктуры сетей. На предприятиях среднего и крупного масштаба применение одного высокотехнологичного решения позволяет значительно уменьшить затраты на содержание более громоздкой и разрозненной архитектуры, созданной на основе различных продуктов, которые зачастую имеют проблемы с взаимодействием между собой. Но совместно с положительными сторонами этих систем можно выделить несколько отрицательных факторов:

- большие финансовые затраты на реорганизацию;
- сложность диагностики аварий;
- необходимость дополнительного обучения персонала.

Учитывая высокую стоимость таких решений, необходимо создать условия для стабильной работы оборудования и исключить возможность выхода его из строя, который приведет к крупным затратам на восстановление.

Решить данные задачи могут системы централизованного мониторинга и управления сетью передачи данных (СПД). Существует множество готовых систем, как свободно распространяемых, так и коммерческих, но прежде чем внедрять какую-либо из них в производственный процесс, необходимо провести тщательный анализ и учесть все риски, связанные с применением таких систем на отдельно взятой инфраструктуре СПД.

Цель данной работы состоит в том, чтобы разработать алгоритм для применения систем централизованного мониторинга и управления, а так же изучить возможность адаптации их к конкретным задачам на предприятии.

Для того что бы внедрить систему в уже действующую инфраструктуру, необходимо учесть несколько параметров. Система должна включать в себя модули позволяющие осуществлять управление сетевым оборудованием, рабочими станциями и серверами, как в ручном режиме, так и автономном. Так же система должна отвечать нескольким требованиям:

- минимальное количество материальных затрат на внедрение;
- высокая безопасность;
- высокая скорость внедрения;
- поддержка современных сетевых протоколов и технологий;
- взаимодействие с имеющимися программными продуктами.

Необходимый функционал систем мониторинга и управления СПД

Таким образом, для основных сетевых службе можно выявить следующий необходимый функционал системы мониторинга и управления (рисунок 1):

- HTTP (англ. HyperText Transfer Protocol — «протокол передачи гипертекста»);
- FTP (англ. File Transfer Protocol — протокол передачи файлов);
- SSH (англ. Secure SHell — «безопасная оболочка»);
- SMB (сокр. от англ. Server Message Block);
- NFS (Network File System);
- SNMP (англ. Simple Network Management Protocol — протокол простого управления сетями);
- POP3 (англ. Post Office Protocol Version 3 — протокол почтового отделения, версия 3);
- RTMP (англ. Real Time Messaging Protocol);
- MySQL (TCP 3306).

Необходимый функционал системы мониторинга для системных ресурсов серверов:

- свободное место на жестком диске;
- оперативная память;
- загрузка CPU;
- использование виртуальной памяти.

Помимо основных ресурсов, некоторым серверам требуется мониторинг специализированных ресурсов:

- состояние RAID массива;
- общее использование ресурсов VPS.

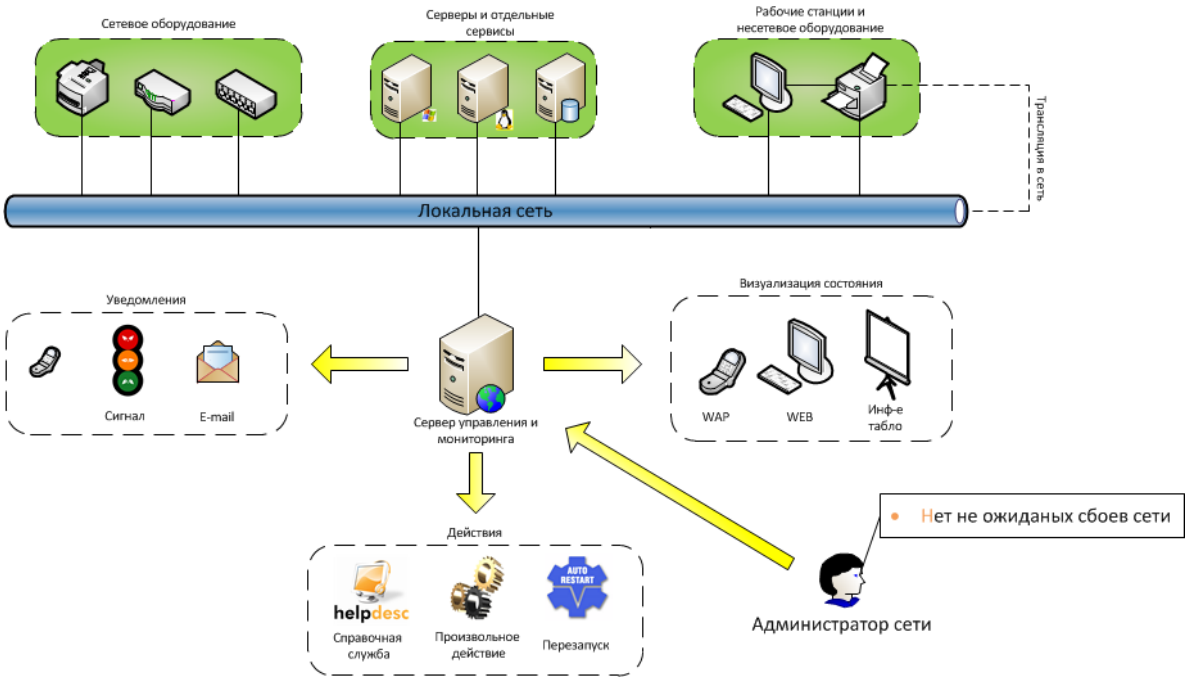

Рисунок 1 – Необходимый функционал

На данный момент существует множество систем мониторинга и управления, позволяющих решать многие проблемы, возникающие при эксплуатации сетевого оборудования. Для сокращения расходов на внедрение таких систем желательно (а в некоторых случаях необходимо) рассматривать программные продукты, работающие

под управлением операционных систем семейства Linux. Для последующего анализа был отобран ряд систем, представленных в таблице 1.

Сравнительный анализ свободно распространяемых систем мониторинга и управления СПД

Таблица 1 – Общие данные по всем системам

Система	Nagios	Icinga	Zabbix	Pandora FMS	GroundWork	PRTG Network Monitor	Zenoss
Диаграммы	Да	Нет	Да	Да	Да	Да	Да
Отчёты SLA	Через плагин	Через плагин	Нет	Да	Через плагин	Да	Да
Логическое группирование	Да	Да	Да	Да	Да	Да	Да
Trending (события)	Да	Да	Да	Да	Нет	Да	Да
Trend Prediction (прогнозирование событий)	Нет	Нет	Да	Да	Нет	Да	Да
Автоматическое обнаружение	Через плагин	Через плагин	Да	Да	Через плагин	Да	Да
Агент	Да	Да	Да	Да	Да	Да	Нет
SNMP	Через плагин	Через плагин	Да	Да	Через плагин	Да	Да
Syslog	Через плагин	Нет	Да	Да	Через плагин	Да	Да
Внешние скрипты	Да	Да	Да	Да	Да	Да	Да
Плагины	Да	Да	Да	Да	Да	Да	Да
Сложность создания плагинов	Легкий	Легкий	Средний	Сложно	Легкий	Сложно	Легкий
Триггеры/ Тревоги	Да	Да	Да	Да	Да	Да	Да
Доступ через Web	Просмотр, Отчёты, Управление	Просмотр, Отчёты, Управление	Полный доступ	Полный доступ	Просмотр, Отчёты, Управление	Полный доступ	Полный доступ
Распределённый мониторинг	Да	Да	Да	Да	Да	Да	Да
Инвентаризация	Через плагин	Через плагин	Да	Да	Через плагин	Да	Да
Метод хранения данных	Плоская база данных, SQL	Плоская база данных, SQL	SQLite, MySQL, PostgreSQL, Oracle	MySQL	Плоская база данных, SQL	SQL	MySQL для событий, Zope для всего остального
Лицензия	GNU GPL	GNU GPL	GNU GPL	GPLv2	GNU GPL	Коммерческая, бесплатная	GNU GPL; (Доступна редакция Enterprise)
Карты	Динамические, настраиваемые	Динамические, настраиваемые	Да	Да	Динамические, настраиваемые	Да	На базе Google Map
Управление доступом	Да	Да	Да	Да	Да	Да	Да
События	Да	Да	Да	Да	Да	Да	Да
Язык	C	C	C	PHP — фронтенд	C	PHP, C	Zope, Python

Очевидно, что не все системы мониторинга и управления в полной мере покрывают необходимый функционал. Для всех программных продуктов, участвующих в анализе, были выявлены основные критерии и записаны в первой колонке таблицы 1.

После проведения сравнительного анализа систем мониторинга и управления видно, что такие системы, как Nagios, Zennos, Zabbix отвечают всем требованиям.

Кроме того, эти системы являются наиболее удобными для создания на их основе собственного решения, так как они:

- позволяют создавать собственные проверки;
- позволяют создавать собственные компоненты;
- позволяют легко интегрировать другие системы;
- являются основой ряда систем мониторинга;
- позволяют создать собственный метод конфигурирования.

После того, как системы централизованного мониторинга и управления на основе Zennos и Nagios были развернуты в режиме тестирования на одном из телекоммуникационных предприятий г. Красноярска удалось автоматизировать следующие процессы:

- мониторинг работоспособности и производительности серверов и отдельных сервисов, а также сетевых устройств;
- оповещения о проблемах технических специалистов, ответственных за соответствующие компоненты информационной инфраструктуры до того, как они нанесли существенный ущерб и повлияли на работу пользователей;
- контроль над состоянием оборудования и расходных материалов;
- учет времени работы и простоя систем, а также возникающих проблем и аварий для последующего анализа;
- реагирование на предсказуемые проблемы без участия людей (например, перезапуск систем или процесса в случае сбоя).

Для осуществления централизованного управления и мониторинга, не было затрачено никаких средств, при этом системы были развернуты на базе свободно распространяемых продуктов, что обеспечило максимально эффективное решение, которое в результате внедрения позволило:

- повысить отказоустойчивость информационной инфраструктуры за счет оперативного, вплоть до фактического возникновения, реагирования на возникающие проблемы;
- повысить эффективность труда сотрудников информационных отделов за счет снижения трудозатрат на поиск проблем и их причин, а также автоматизации ряда рутинных операций;
- снизить эксплуатационные расходы за счет минимизации ущерба от возникающих проблем, сокращения числа сбоев и отсутствия лицензионных платежей за право использования решения;
- обоснованно выделять денежные средства на модернизацию оборудования и программного обеспечения с учетом имеющейся статистики отказов, а также загрузки ресурсов оборудования и результатов анализа их причин.

Список использованной литературы

1. Олифер, В. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / Виктор Олифер, Наталия Олифер. - 4-е изд. - СПб. : Питер, 2011. - 944 с. : ил.; 70x100/16. - 4500 экз.

2.Nagios - The Industry Standard in IT Infrastructure Monitoring [Электронный ресурс] Официальный сайт сообщества разработчиков системы управления и мониторинга Nagios - Режим доступа: http://www.nagios.org. – Загл. с экрана.

3. Zenoss The Cloud Management Company [Электронный ресурс] Управляющая компания Zenoss - Режим доступа: http://www.zenoss.com. – Загл. с экрана.