Рунышков И.Н. Обзор средств сетевого мониторинга вычислительных сетей и оборудования в их составе // Академия педагогических идей «Новация». Серия: Студенческий научный вестник. – 2017. – № 05 (май). – АРТ 288-эл. – 0,2 п.л. - URL: <http://akademnova.ru/page/875550>

РУБРИКА: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.031.6

Рунышков Иван Николаевич
студент 1 курса, институт заочного и дистанционного образования
ФГБОУ ВО «Московский технологический университет» МИРЭА
г. Москва, Российская Федерация
e-mail: mail4tol@gmail.com

ОБЗОР СРЕДСТВ СЕТЕВОГО МОНИТОРИНГА ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ И ОБОРУДОВАНИЯ В ИХ СОСТАВЕ

Аннотация: в статье рассмотрены современные методы мониторинга сетей.

Ключевые слова: мониторинг, вычислительные сети, система мониторинга оборудования.

Runyshkov Ivan
1st year student, institute of correspondence and distance education
FGBOU VO «Moscow University of Technology» MIREA
Moscow, Russian Federation

REVIEW OF MEANS OF NETWORK MONITORING OF COMPUTER NETWORKS AND EQUIPMENT IN THEIR COMPOSITION

Abstract: In the article, modern methods of network monitoring are considered.

Keywords: Monitoring, computer networks, equipment-monitoring system.

Любая сложная вычислительная сеть требует дополнительных специальных средств управления помимо тех, которые имеются в стандартных сетевых операционных системах. Это связано с большим количеством разнообразного коммуникационного оборудования, работа которого критична для выполнения сетью своих основных функций. Распределенный характер крупной корпоративной сети делает невозможным поддержание ее работы без централизованной системы управления, которая в автоматическом режиме собирает информацию о состоянии каждого концентратора, коммутатора, мультиплексора и маршрутизатора и предоставляет эту информацию оператору сети. Обычно система управления работает в автоматизированном режиме, выполняя наиболее простые действия по управлению сетью автоматически, а сложные решения предоставляя принимать человеку на основе подготовленной системой информации. Система управления должна быть интегрированной. Это означает, что функции управления разнородными устройствами должны служить общей цели обслуживания конечных пользователей сети с заданным качеством.

Постоянный контроль за работой локальной сети, составляющей основу любой корпоративной сети, необходим для поддержания ее в работоспособном состоянии. Контроль — это необходимый первый этап, который должен выполняться при управлении сетью. Ввиду важности этой функции ее часто отделяют от других функций систем управления и реализуют специальными средствами. Такое разделение функций контроля и собственно управления полезно для небольших и средних сетей, для

которых установка интегрированной системы управления экономически нецелесообразна. Использование автономных средств контроля помогает администратору сети выявить проблемные участки и устройства сети, а их отключение или реконфигурацию он может выполнять в этом случае вручную.

Процесс контроля работы сети обычно делят на два этапа — мониторинг и анализ.

На этапе мониторинга выполняется более простая процедура — процедура сбора первичных данных о работе сети: статистики о количестве циркулирующих в сети кадров и пакетов различных протоколов, состоянии портов концентраторов, коммутаторов и маршрутизаторов и т. п.

Далее выполняется этап анализа, под которым понимается более сложный и интеллектуальный процесс осмысления собранной на этапе мониторинга информации, сопоставления ее с данными, полученными ранее, и выработки предположений о возможных причинах замедленной или ненадежной работы сети.

Задачи мониторинга решаются программными и аппаратными измерителями, тестерами, сетевыми анализаторами, встроенными средствами мониторинга коммуникационных устройств, а также агентами систем управления. Задача анализа требует более активного участия человека и использования таких сложных средств, как экспертные системы, аккумулирующие практический опыт многих сетевых специалистов.

Мониторинг компонентов вычислительной сети условно можно разделить на следующие категории:

1) мониторинг и анализ эффективности выполнения программ в вычислительной сети (контроль текущего состояния вычислительных

процессов и их отдельных экземпляров, оценка эффективности использования выделенных ресурсов);

2) мониторинг, тестирование и диагностика аппаратных компонентов вычислительных узлов (жесткие диски, процессоры, оперативная память, сетевые интерфейсы и др.);

3) мониторинг инженерной инфраструктуры вычислительной сети (системы бесперебойного питания, климатическое оборудование, системы пожаротушения и др.);

4) мониторинг вычислительной инфраструктуры вычислительной сети (мониторинг текущей загрузки вычислительных узлов, контроль коммуникационных, управляющих и сервисных сетей, систем хранения данных);

5) мониторинг промежуточного программного обеспечения вычислительной сети (мониторинг функционирования системных служб, очередей задач, агентов, различных подсистем и др.).

В категории средств мониторинга и анализа эффективности выполнения программ в вычислительной сети накоплено несколько десятков профилировщиков программ, средств мониторинга загрузки вычислительных ресурсов экземплярами программ, выполняемых в узлах вычислительной сети, средств мониторинга загрузки сетевых компонентов и т.д. Среди наиболее популярных и широко используемых средств можно выделить следующие:

– NWPerf – система анализа эффективности выполнения параллельных программ в крупномасштабных ВВС с возможностью предоставления данных как по всей параллельной программе в целом, так и по ее отдельным экземплярам.

– Allinea MAP – профилировщик параллельных, многопоточных и последовательных программ, предоставляющий исчерпывающий анализ по множеству метрик.

– Lapta – инструментарий для многоаспектного анализа динамических характеристик параллельных программ, выполняемых на суперкомпьютерах.

– mpiP – легковесный профилировщик MPI-программ.

– IPM – расширенный профилировщик параллельных программ с возможностью анализа MPI-пересылок, доступа к памяти, работе с сетевыми интерфейсами, диском.

– Intel VTune – инструментарий для анализа производительности, масштабируемости, пропускной способности, кэширования при выполнении программ в вычислительной сети.

– HPCToolkit – инструментарий для мониторинга выполнения параллельных программ с возможностью анализа используемых ресурсов, автоматического выявления неэффективных блоков с привязкой к исходному тексту программы.

– Paraver – анализатор производительности программ, основанный на трассировке событий и позволяющий производить детальный анализ изменения и распределения метрик с целью понимания поведения приложений.

– Scalasca – инструментарий для выполнения оптимизации параллельных программ путем измерения и анализа их поведения во время выполнения.

Из представленного списка наиболее функциональными и перспективными решениями для анализа эффективности выполнения

параллельных программ в вычислительной сети, являются пакеты с открытым исходным кодом NWPperf и Paraver.

При мониторинге, тестирование и диагностика аппаратных компонентов вычислительных узлов, для выявления неисправностей в аппаратных компонентах вычислительных узлов вычислительной сети, заслуживающими внимания являются:

– Disparity – подход, основанный на запуске MPI-программы на анализируемых узлах с целью обнаружения возможных неисправностей.

– CIFTS – использует механизмы обмена информацией о неисправностях с целью выработки целостной картины о состоянии узлов.

Для мониторинга инженерной инфраструктуры суперкомпьютерных центров и центров обработки данных наиболее распространенными средствами являются: ClustrX, EMC ViRP SRM, HP Cluster Management Utility, Bright Cluster Manager, Moab Adaptive HPC Suite, IBM cluster system management. Однако все перечисленные средства являются проприетарными, зачастую жестко привязаны к оборудованию и не всегда обладают достаточной гибкостью для мониторинга инфраструктуры разнородных вычислительных сред.

Среди некоммерческих продуктов авторам не удалось найти приемлемых средств, которые позволяли бы универсально описывать состав разнородного инженерного оборудования суперкомпьютерного центра, создавать новые объекты и задавать правила их мониторинга. Системы мониторинга Nagios, Zabbix предоставляют набор средств для мониторинга инфраструктуры вычислительной сети, которые в каждом отдельном случае необходимо существенно дорабатывать.

В категории мониторинга вычислительной инфраструктуры вычислительной сети на сегодняшний день существует значительное число комплексных решений. Наиболее популярными из них являются:

- Ganglia – масштабируемая распределенная система мониторинга кластеров параллельных и распределенных вычислений и облачных систем с иерархической структурой;

- Nagios – система мониторинга вычислительных систем и сетей с широкими возможностями уведомления оператора о возможных неисправностях;

- Zabbix – система мониторинга и отслеживания состояния разнообразных сервисов компьютерной сети, серверов и сетевого оборудования;

- ZenOSS – система мониторинга с возможностями автоматического обнаружения и конфигурирования параметров контроля различных систем;

- Ovis2 – комплексная система мониторинга, обеспечивающая высокую масштабируемость и интеграцию с другими системами мониторинга.

Наиболее популярной системой в данной категории по-прежнему является система мониторинга Ganglia. Однако стандартный набор функций данной системы не обеспечивает возрастающих потребностей по мониторингу вычислительного оборудования, что зачастую приводит к необходимости использования дополнительных систем мониторинга, таких как Zabbix или Nagios. Наиболее перспективной системой в данной категории, является система Ovis2, обеспечивающая высокую масштабируемость и широкие возможности по подключению различных источников данных.

В категории мониторинга промежуточного программного обеспечения вычислительной сети могут использоваться как описанные выше системы мониторинга Nagios и Zabbix, так и более специализированные средства, такие как:

- Хумон – мониторинг работы системных сервисов;
- FATE – инструментарий тестирования облачных приложений;
- CloudRift – среда тестирования микросервисных приложений.

Кроме перечисленных средств, администраторами вычислительной сети зачастую разрабатываются специализированные утилиты для отслеживания корректного функционирования отдельных подсистем, входящих в состав промежуточного ПО вычислительной сети, зачастую реализуемые в виде скриптов, запускаемых по расписанию с использованием сервиса CRON.

Список использованной литературы:

1. Электронный ресурс: Лекции А.Н. Самойлова по Системам и Сетям Передачи Данных
<http://seticom.narod.ru/lit/12sdl-01.htm>
2. Электронный ресурс: Анализ современных систем мониторинга
<https://cyberleninka.ru/article/n/analiz-sovremennyh-sistem-monitoringa>
3. Электронный ресурс: Актуальность современных систем удаленного мониторинга вычислительных ресурсов
<https://cyberleninka.ru/article/n/aktualnost-sovremennyh-sistem-udalennogo-monitoringa-vychislitelnyh-resursov>

Дата поступления в редакцию: 21.06.2017 г.

Опубликовано: 21.06.2017 г.

***© Академия педагогических идей «Новация». Серия «Студенческий научный вестник»,
электронный журнал, 2017***

© Рунышков И.Н., 2017

Всероссийское СМИ

«Академия педагогических идей «НОВАЦИЯ»

Свидетельство о регистрации Эл №ФС 77-62011 от 05.06.2015 г.

(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru

e-mail: akademnova@mail.ru

Для заметок