

Мухаметзянов М.Р.

магистр

Научный руководитель: доцент Андреев В. В.

Казанский Государственный Энергетический Университет

ТЕЛЕМЕТРИЯ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Аннотация.

В этой статье мы рассмотрим основы телеметрии приложения, его среды и компонентов. Так же приведем базовую стратегию реагирования на результаты телеметрии.

Ключевые слова: информационные системы, телеметрия, мониторинг

Annotation.

In this article, we will look at the base of the application's telemetry, its environment, and components. We will also give a basic strategy to respond to the results of telemetry.

Keywords: information systems, telemetry, monitoring

Введение.

Телеметрия – это совокупность методов сбора информации и измерения параметров, позволяющая получить необходимые сведения об удаленных объектах [1].

В мире разработки программного обеспечения телеметрия может дать представление о том, какие функции конечные пользователи используют чаще всего, обнаруживать ошибки и проблемы, а также дает информацию о производительности систем.

Серверная прикладная телеметрия

Чтобы обеспечить приемлемое время безотказной работы и производительность необходимо начать мониторинг с составляющих вашей системы. В первую очередь, с физических серверов. Мониторинг серверов и

мониторинг компьютеров в целом требуют достаточное количество телеметрии, поэтому она должна быть в центре внимания.

Помимо указания того, работает ли сервер или нет, необходимо включить в телеметрию загрузку ЦП сервера, включая пики и средние значения за различные периоды времени. Нужно обратить внимание на очевидное чрезмерное использование, но также и не забывать, что недостаточное использование ресурсов процессора может указывать на проблемы. Например, недостаточное использование может указывать на проблему сетевой маршрутизации. Также нужно реализовать возможность просмотреть статистику отдельных серверов, а также статистику по группам серверов, чтобы понять, является ли загрузка ЦП системной проблемой (например, общая нагрузка на сервер приложений) или указывает на подмножество серверов, которые находятся в определенной группе (например, старое оборудование) или сервер, который собирается выйти из строя.

Другая телеметрия для мониторинга включает использование памяти сервера и загрузку ввода-вывода с течением времени. Это важно в средах, где интенсивно используется виртуализация серверов. В таких случаях статистика, сообщаемая с виртуальных серверов, может указывать не на проблемы использования ЦП или памяти, а на то, что базовые физические серверы могут быть переподписаны с точки зрения виртуализации, ЦП, связи ввода-вывода с дисками и периферийными устройствами или нехватки физической памяти. Наконец, специфичные для сервера измерения должны включать пользовательские запросы во времени, а также одновременную активность пользователей, указанную в графиках стандартных отклонений. Это даст не только информацию о производительности сервера, но и общую нагрузку на систему.

Телеметрия инфраструктуры приложения

Теперь, когда мы рассмотрели серверы и телеметрию их физических компонентов, можно немного глубже рассмотреть некоторые основополагающие компоненты построения вашего приложения, которые включают в себя сетевую инфраструктуру, инфраструктуру хранения, а также общую пропускную способность и потребление.

Понимание теоретических и практических ограничений сегментов сети имеет решающее значение для понимания того, когда пакеты будут потеряны и когда могут возникнуть «сетевые штормы». Например, когда вы приближаетесь к пределу пропускной способности сегмента локальной сети, UDP-сообщения

будут потеряны, а потерянные TCP/IP-сообщения будут переданы повторно, что потенциально увеличивает проблему. Мониторинг сети должен выявить использование полосы пропускания сегмента с течением времени в разных областях сети (например, между серверами приложений и серверами баз данных). Кроме того, специфический для протокола мониторинг сети предоставит более детальное представление об использовании приложений и, возможно, проблемах производительности для определенных областей функциональности (таких как трафик HTTP/S или трафик внутренней базы данных). Кроме того, запросы мониторинга к определенным сетевым портам могут точно определить потенциальные дыры в безопасности, а также задержки маршрутизации и переключения в соответствующих сетевых компонентах.

Основное применение телеметрии

Сосредоточив внимание на самом приложении, важно отслеживать некоторые ключевые телеметрии, которые могут включать доступ к базе данных и ее обработку. С точки зрения доступа очень важно следить за количеством открытых соединений с базой данных, которые могут взлететь и повлиять на производительность. Причины этого включают большие (и растущие) пулы физических и виртуальных серверов приложений, ошибки программирования и неправильную настройку сервера приложений. Отслеживание этого с течением времени может указать на принятые ранее проектные решения, которые не масштабируются по мере увеличения использования приложений. С точки зрения обработки базы данных важно отслеживать количество запросов к базе данных, их время отклика и количество данных, передаваемых между базой данных и приложениями. Это должно включать как средние, так и выбросы. Иногда задержка может быть скрыта или затенена, если смотреть только на средние значения, но эти выбросы могут напрямую влиять и раздражать ваших пользователей.

Что касается ошибок, ваша стратегия мониторинга должна учитывать исключения приложений, ошибки базы данных или предупреждения, журналы сервера приложений для необычной активности (чрезмерная сборка мусора Java), веб-журналы, указывающие на запросы, и так далее. Это начало мониторинга индикаторов безопасности в вашем приложении.

Инструменты и стратегия

Иметь стратегию мониторинга важно, но также необходимо иметь хорошо спланированную стратегию реагирования, которая включает в себя следующее:

- Обнаружение первого уровня для выявления, понимания и начала анализа причины проблемы.
- Документированный план коммуникации, который включает имена и контактную информацию руководителей или руководителей, которые могут быстро принимать соответствующие деловые и технологические решения.
- Краткосрочные исправления, которые вы можете быстро определить для восстановления приложения.
- План расследования будущего уклонения (начиная с плана долгосрочного решения).

Для упрощения работы с данными телеметрии можно пользоваться дополнительными набором инструментов, который включает в себя:

- Панели мониторинга или другие инструменты визуализации для системной телеметрии и отчетности в режиме реального времени.
- Инструменты бизнес-аналитики для поиска скрытой информации, такой как сезонные схемы использования или реакции на изменения.
- Инструменты автоматизации, которые устраняют ручную работу, с автоматическим обнаружением, восстановлением и снижением рисков.
- Аналитика безопасности: расширенный анализ угроз, который ищет подозрительную активность пользователя, доступ к внешней сети, необычную активность в базе данных и т. д., чтобы обнаружить инциденты взлома до того, как они станут угрозой безопасности.

Работа со средствами телеметрии не только поможет реализовать надежную стратегию мониторинга, но также обеспечит ее развитие и расширение с течением времени.

Использованные источники:

1. Телеметрия | Телеизмерение [Электронный ресурс] // Новософт Глоссарий. – URL: <http://www.novosoft.ru/glossary/telemetriya.shtml> (дата обращения: 15.05.2020).
2. Telemetry and Feedback [Электронный ресурс] // Log Management & Security Analytics, Continuous Intelligence | Sumo Logic. – URL: <https://www.sumologic.com/insight/devops-telemetry-feedback/> (дата обращения: 15.05.2020).
3. IT Безопасность. Телеметрия [Электронный ресурс] // Medium. – URL: https://medium.com/@fck_rkn/fcd957a93a02 (дата обращения: 15.05.2020).
4. Global Airborne Telemetry Market- Industry Trends and Forecast to 2025 [Электронный ресурс] // Market Prognosis. – URL:

<https://marketprognosis.com/report/global-airborne-telemetry-market--industry-trends-and-forecast-to-2025/pr-15421> (дата обращения: 15.05.2020).

5. What is Telemetry? The Guide to Application Monitoring [Электронный ресурс] // Log Management & Security Analytics, Continuous Intelligence | Sumo Logic. – URL: <https://www.sumologic.com/insight/what-is-telemetry/> (дата обращения: 17.05.2020).