Инженерный вестник Дона, №2 (2024)
ivdon.ru/ru/magazine/archive/n2y2024/9028

Системы мониторинга ИТ-инфраструктуры на основе больших данных

А.С. Каменев

Государственный университет «Дубна», г. Дубна, Россия

Аннотация: В статье рассматривается активно формирующийся в последнее десятилетие новый класс систем мониторинга ИТ-инфраструктуры, ключевой особенностью которого является широкое использование методов и техник работы с большими данными. Изучаемые системы в зависимости от рыночного позиционирования известны под такими названиями как AIOps, observability platform, all-in-one monitoring, зонтичный мониторинг. В своем обзоре существующих зарубежных и отечественных коммерческих решений авторы делают упор на использование в них методов работы с большими данными. На основе обзора предлагается классификация таких продуктов, позволяющая упорядочить существующее многообразие и выбрать наиболее подходящую систему для стоящих перед организацией задач в области мониторинга все усложняющейся ИТ-инфраструктуры. Актуальность исследования обусловлена отсутствием классификации исследуемых объектов в виду их относительной новизны и ярко выраженного практического характера.
Ключевые слова: система мониторинга, ИТ-инфраструктура, зонтичный мониторинг, AIOps, большие данные, машинное обучение.

Введение

Средства мониторинга ИТ-инфраструктуры можно отнести к одним из самых динамично развивающихся и передовых классов программного обеспечения на протяжении всего существования информационных технологий как отдельной отрасли. Появление новых технологий приводит к усложнению ИТ-инфраструктуры и увеличению ее охвата и глубины внедрения в остальные сферы жизни, и требует развития средств мониторинга и контроля работоспособности, как функционально (поддержка новых технологий, протоколов), так и качественно (обработка большего объема данных мониторинга, скорость реагирования, надежность, территориальная распределенность) [1]. Ярким примером может служить инструмент Prometheus, разработанный для поддержки технологий контейнеризации приложений [2] и активно применивший технологии TSDB и новые подходы в формировании порогов временных рядов. Примечательно, что Prometheus был вторым запущенным проектом фонда CNCF Linux Foundation после Kubernetes, основной технологии

контейнерных приложений [3]. Таким образом, средства мониторинга неизбежно вбирают в себя достижения и самые современные решения отрасли, и зачастую разрабатываются параллельно с ними.

Динамизм неизбежно порождает все более углубляющуюся дифференциацию средств мониторинга. Нередко в рамках одного предприятия сосуществуют классические средства мониторинга сетей и серверов, системы сбора логов, средства мониторинга контейнеризированных приложений, системы мониторинга производительности приложений, средства роботизированного тестирования и т.д. [4, 5]. Для централизованного управления и взаимодействия с таким разнообразным ландшафтом в последнее десятилетие появился целый ряд продуктов. В зависимости от функционального акцента, эти продукты можно встретить под такими ярлыками, как AIOps (Artificial Intelligence for IT Operations), observability platforms, all-in-one monitoring или встречающийся на российском рынке зонтичный мониторинг. На наш взгляд, единство цели и методов позволяет объединить все эти продукты в отдельный класс: систем мониторинга ИТ-инфраструктуры на основе больших данных.

Терминология и рыночное позиционирование

Как это часто бывает на практике, при формировании нового класса программных продуктов маркетинговая активность разработчиков вкупе с децентрализацией и параллельной разработкой решений вносят изрядную долю энтропии в еще несформировавшуюся терминологию.

Первопроходцами сегмента можно считать компании HP и IBM, которые в 2013 г. сформулировали проблему мониторинга гетерогенных сред, прежде всего облачных, и анонсировали ее решение в своих продуктах корпоративного мониторинга: HP Business Service Management и IBM Tivoli, соответственно [6, 7]. В 2016 г. в официальном русскоязычном блоге компании HP появляется термин зонтичный мониторинг [8]. В конце 2017 г.

аналитическое агентство Gartner, исходя из перспектив применения технологий искусственного интеллекта в мониторинге ИТ, вводит в оборот термин AIOps (artificial intelligent for IT operations) для подобных решений [9]. Несмотря на первоначальный успех термина AIOps, позже, ввиду возникших сложностей при внедрении технологий ИИ на практике и неверно формирующихся ожиданий потребителей, ряд вендоров отошел от активного использования данного термина, предпочитая ему более широкое определение observability platform [10]. Даже автора термина, агентство Gartner, возникший сегмент рынка в настоящее время обозначает как «APM and observability tools», объединяя его со средствами контроля производительности приложений. При этом уникальным и устойчивым остается не встречающийся в англоязычной среде российский термин «зонтичный мониторинг».

Базовой технологией, повсеместно встречающейся во всех подпадающих под обозначенные термины решениях, является сбор данных с других программных продуктов и первичных средств мониторинга и массово-параллельная обработка их в режиме реального времени. При этом определяющие характеристики, а также проблемы лежат в области «трех V» (volume, velocity, variety), свойственных технологиям больших данных. Практически у всех решений используются в том или ином виде технологии больших данных: NoSQL СУБД, брокеры сообщений (Apache Kafka, RabbitMQ), программные каркасы типа Apache Hadoop. Таким образом, на наш взгляд, сформировавшиеся за последнее 10 лет программные продукты можно обозначать как системы мониторинга ИТ-инфраструктуры на основе больших данных, а ключевым признаком включения в этот сегмент считать использование технологических решений больших данных.

Сформированный на основании этого критерия перечень основных представителей класса приведен в таблице 1.

Таблица 1.

Перечень систем мониторинга на основе больших данных

№ п/п	Группа	Наименование	Разработчик
1.1	I	DX Operational Intelligence	Broadcom (США)
1.2		Operations Bridge	Microfocus (Великобритания)
1.3		Watson AIOps	IBM (США)
2.1	II	AppDynamics	Microsoft (США)
2.2		Dynatrace	Dynatrace (США)
2.3		New Relic	New Relic (США)
2.4		Instana	Instana (ФРГ)
3.2	III	Humio	CrowdStrike Holdings (США)
3.3		Splunk	Splunk (США)
3.4		Elastic Search	Elastic N.V. (Нидерланды)
4.1	IV	Monq	Монк Диджитал Лаб (Россия)
4.2		PagerDuty	PagerDuty (США)
4.3		Moogsoft	Moog Software (США)
4.4		BigPanda	BigPanda (США)
4.5		DataDog	DataDog (США)

Классификация

Несмотря на единство цели (централизации мониторинга гетерогенных сред) и использование в своей основе методов и техник больших данных, представленные на рынке решения все же имеют ряд отличий, позволяющих провести их классификацию.

На наш взгляд, отличия вызваны, прежде всего, историческим процессом формирования и развития данных продуктов, своеобразным «онтогенезом». Применяя этот подход, мы предлагаем выделить четыре группы.

Группа I. Зонтичный мониторинг для корпоративного ПО в линейке крупного вендора. Самая старая и функционально зрелая группа. Крупные игроки (HP, IBM, Cisco) за свою историю предлагали большое количество различных решений по мониторингу и эксплуатации ИТ, при этом часть этих решений появились в результате слияний и поглощений, т.е. изначально программные продукты развивались самостоятельно и не имели единого технологического каркаса. Что в итоге потребовало наличия единого интерфейса и средства управления «разношерстным» ПО, в результате слияний и поглощений оказавшегося в единой технологической линейке. Таким образом, с проблемой обеспечения синхронизации разнообразных средств мониторинга крупные разработчики корпоративного ПО встретились намного раньше, чем даже их клиенты. Отсюда следуют основные достоинства и недостатки систем из этой группы. Главным преимуществом является наиболее полное функциональное покрытие. Но это преимущество возникает зачастую только в случае использования в качестве средств мониторинга и эксплуатации ИТ всей линейки от одного производителя. Со сторонними продуктами представители данной группы либо несовместимы, либо не раскрывают в полной мере заявленный функционал, что требует долгосрочных и дорогих проектов по переводу всей инфраструктуры на решения от единого вендора.

Группа II. Application Performance Monitoring (APM). Системы мониторинга производительности приложений. Данная группа изначально развивалась и по большей части развивается как системы мониторинга производительности приложений со всеми вытекающими атрибутами: исключительно агентский мониторинг, встраивание в код исполняемых приложений специальных участков. Основным преимуществом является возможность сбора информации со всех слоев исполнения приложения, что дает такой важный функционал как построение в автоматическом режиме

топологии приложения. Основной недостаток - стоимость и трудозатраты при внедрении. Трудностей добавляют несовместимые агенты и протоколы работы с телеметрией АРМ от разных вендоров. Однако стоит отметить, что в последнее время осуществляются активные попытки решить данную проблему универсализации, ярким примером чего может служить стартовавший в 2019 г. проект OpenTelemetry от CNCF.

Группа III. Системы сбора и мониторинга логов. Очень гибкие системы по сбору различной текстовой информации из самых разнообразных источников. Предназначены для сбора, обработки и аналитики больших объемов данных. Ядром данных продуктов является специализированная СУБД, движок ETL и язык запросов.

Группа IV. Системы управления алертами. Самая молодая группа продуктов, объединенная подходом сбора аварийных событий с промежуточных классических систем мониторинга с последующей обработкой и автоматизацией действий команд. Главные задачи - снижение шума, вызванного множественными алертами, и автоматизация работы дежурных служб. Основным преимуществом является возможность работы с уже существующими в организации системами мониторинга без серьезного перестроения служб. Стоит отметить, что системы управления алертами являются надстройкой над существующим ландшафтом, поэтому эффективность внедрения пропорциональна зрелости процессов мониторинга и эксплуатации ИТ.

Представители соответствующих классификационных групп приведены в Табл. 1.

Заключение

Системы мониторинга служат индикатором прогресса отрасли в целом. В данном сегменте в последнее десятилетие можно выявить две взаимосвязанные тенденции: 1) дифференциация, когда в пределах ИТ-

инфраструктуры одного крупного предприятия активно используются десятки различных специализированных инструментов ИТ-мониторинга; 2) появление и развитие средств мониторинга на основе методов и практик больших данных, вызванное необходимостью объединения, нормализации и обработки информации от дифференцированных инструментов.

Предлагаемая в статье классификация позволяет выделить основные пути развития и особенности активно формирующегося класса решений мониторинга на основе больших данных и может быть полезна как при проектировании отечественных аналогичных систем, так и при внедрении уже существующих решений на предприятии.

Литература

1. Серрано Н., Эрнантес Х., Галлардо Г. Средства мониторинга ИТ-инфраструктуры // Электронная версия журнала «Открытые системы. СУБД». 2015. № 04. URL: osp.ru/os/2015/04/13047967.

2. Лазарева Н.Б. Автоматизация развертывания Kubernetes-кластеров на базе Ubuntu ОС в Rancher на инфраструктуре VMWare vSphere // Инженерный вестник Дона. 2023. №4. URL: ivdon.ru/ru/magazine/archive/n4y2023/8325.

3. Kristen Evans Cloud Native Computing Foundation Announces Prometheus Graduation (09.08.2018) // cncf.io. URL: cncf.io/announcements/2018/08/09/prometheus-graduates/ (дата обращения: 15.01.2024).

4. Верещагина Е.А., Рудниченко А.К., Колесникова Д.С. Windows Management Instrumentation как способ мониторинга и аудита ИТ-инфраструктуры предприятия // Инженерный вестник Дона. 2019. №8. URL: ivdon.ru/ru/magazine/archive/N8y2019/6125.

5. Ревнивых А.В., Федотов А.М. Мониторинг информационной инфраструктуры организации // Вестник НГУ. Серия: Информационные

технологии. 2013. №4. URL: cyberleninka.ru/article/n/monitoring-informatsionnoy-infrastruktury-organizatsii.

6. Patrick Thibodeau HP's system tools can now manage public cloud (09.06.2010) // InfoWorld URL: infoworld.com/article/2627152/hp-s-system-tools-can-now-manage-public-cloud.html (дата обращения: 15.01.2024).

7. SaroJ Kar A Name Change for Tivoli Proves New Focus on Smarter Infrastructure | #IBMEdge (24.06.2013) // SiliconANGLE URL: siliconangle.com/2013/06/24/a-name-change-for-tivolis-shows-the-changing-focus-on-smarter-infrastructure-ibmedge/ (дата обращения: 15.01.2024).

8. Зонтичный мониторинг ИТ-ресурсов // Habr (Блог компании Hewlett Packard Enterprise) URL: habr.com/ru/companies/hpe/articles/278883/ (дата обращения: 15.01.2024).

9. Маколей Т. Что такое AIOps и как это работает // Директор информационной службы. 2018. № 5. URL: osp.ru/cio/2018/05/13054534 (дата обращения: 15.01.2024).

10. Шайер Р. Три области, в которых AIOps преуспевает, и две, в которых еще нет // БИТ. Бизнес & Информационные технологии. 2022. № 1(114). С. 30-33.

References

1. Serrano N., Ernantes Kh., Gallardo G. Elektronnaya versiya zhurnala «Otkrytye sistemy. SUBD». 2015. № 04. URL: osp.ru/os/2015/04/13047967

2. Lazareva N.B. Inzhenernyj vestnik Dona. 2023. №4. URL: ivdon.ru/ru/magazine/archive/n4y2023/8325

3. Kristen Evans. Cloud Native Computing Foundation Announces Prometheus Graduation (08/09/2018). cncf.io. URL: cncf.io/announcements/2018/08/09/prometheus-graduates/ (accessed: 01/15/2024).

4. Vereshchagina E.A., Rudnichenko A.K., Kolesnikova D.S. Inzhenernyj vestnik Dona. 2019. №8. URL: ivdon.ru/ru/magazine/archive/N8y2019/6125.

5. Revnivykh A.V., Fedotov A.M. Vestnik NGU. Seriya: Informatsionnye tekhnologii. 2013. №4. URL: cyberleninka.ru/article/n/monitoring-informatsionnoy-infrastruktury-organizatsii.

6. Patrick Thibodeau HP's system tools can now manage public cloud (06/09/2010). URL: infoworld.com/article/2627152/hp-s-system-tools-can-now-manage-public-cloud.html (accessed: 01/15/2024).

7. SaroJ Kar A Name Change for Tivoli Proves New Focus on Smarter Infrastructure | #IBMEdge (06/24/2013). URL: siliconangle.com/2013/06/24/a-name-change-for-tivolis-shows-the-changing-focus-on-smarter-infrastructure-ibmedge/ (accessed: 01/15/2024).

8. Zontichnyj monitoring IT-resursov [Umbrella monitoring IT resources]. Habr (Blog Hewlett Packard Enterprise). URL: habr.com/ru/companies/hpe/articles/278883/ (accessed: 01/15/2024).

9. Makoley T. Direktor informatsionnoy sluzhby. 2018. № 5. URL: osp.ru/cio/2018/05/13054534 (accessed: 01/15/2024).

10. Shayer R. BIT. Biznes & Informatsionnye tekhnologii. 2022. № 1(114). pp. 30-33.

Дата поступления: 10.01.2024

Дата публикации: 15.02.2024