DOI 10.37882/2223–2966.2020.05.34

СЕТЕВОЙ МОНИТОРИНГ: АНАЛИЗ СЕТЕВОГО ТРАФИКА С ПОМОЩЬЮ ELK

NETWORK MONITORING: NETWORK TRAFFIC ANALYSIS USING ELK

V. Petrov
K. Bryukhanov
E. Avksentieva

Summary. A method of network monitoring based on network traffic analysis is proposed. This paper discusses the concept of network monitoring, what are the methods of network monitoring and how to use the elk stack to collect, process and analyze network traffic. As a research method, testing was chosen based on the architecture that was designed and put into operation in the company Dino Systems. This type of architecture can be used for building and implementing network monitoring. The result of the research is the proposed method and approaches to implementing network monitoring.

Keywords: ELK stack, network traffic analysis, network monitoring

Петров Валерий Владимирович
Аспирант, Университет ИТМО, г. Санкт-Петербург
mu_valera@mail.ru
Брюханов Константин Владимирович
Аспирант, Университет ИТМО, г. Санкт-Петербург
devops.spb@gmail.com
Авксентьева Елена Юрьевна
К.п.н., доцент, Университет ИТМО, г. Санкт-Петербург
avksentievaelena@rambler.ru

Аннотация. Предложен метод сетевого мониторинга на основе анализа сетевого трафика. В работе рассмотрено понятие сетевого мониторинга, какие бывают методы сетевого мониторинга и как с помощью стека ELK собирать, обрабатывать и анализировать сетевой трафик. В качестве метода исследования была выбрана апробация на основании архитектуры, которая была спроектирована и введена в эксплуатацию в компании Dino Systems. Данный вид архитектуры может применяться для построения и реализации сетевого мониторинга. Результатом исследования является предложенный метод и подходы к реализации сетевого мониторинга.

Ключевые слова: стек ELK, анализ сетевого трафика, сетевой мониторинг.

Введение

Сетевой мониторинг — это наблюдение за работой сети с целью своевременного обнаружения в ней неисправностей и ошибок. С точки зрения мониторинга, компьютерная сеть состоит из следующих объектов: сетевое оборудование, сетевые соединения, сетевой трафик, сетевые сервисы, и пользователи [2].

Целью данного исследования является раскрытие темы сетевого мониторинга, какие инструменты применяются для организации и какие проблемы есть на данный момент в сетевом мониторинге.

В качестве инструментов для анализа сетевого трафика был выбран стек ELK в связи с тем, что: он полностью свободно распространяется, имеет возможность к горизонтальному масштабированию, имеет высокую доступность, обладает необходимой гибкостью в настройке, а также, имеет два типа сетевого мониторинга. Это NetFlow аналитика, и аналитика сетевых пакетов.

Для достижения цели необходимо:

1. Изучить особенность анализа сетевого трафика в различных условиях
2. Изучить научно-техническую литературу для определения сетевого мониторинга, перспективы использования инструментов для анализа сетевого трафика
3. Проанализировать практический опыт коллег в области сетевого мониторинга для проектирования архитектуры анализа сетевого трафика
4. Разработать архитектуру системы сетевого мониторинга и тестовый стенд для апробации данной архитектуры

Обзор предметной области:

Сетевой мониторинг делится на две части: мониторинг сетевого оборудования, и мониторинг сетевого траффика. В свою очередь, анализ сетевого трафика делится на:

- Анализ пакетов
- Анализ Netflow

Для анализа пакетов сетевого трафика могут быть использованы следующие программные продукты: Wireshark, tcpdump, kismet, EnterApe и др. Принцип их работы заключается в прослушивании трафика, который проходит через сетевое устройство. Но такой вариант

Таблица 1

Инструмент сетевого мониторинга	Критерии								
	1	2	3	4	5	6	7	8	9
Tcpdump	+	+	-	-	-	-	+	-	-
Wireshark	+	+	-	-	-	-	+	+	-
ELK Netflow	+	+	+	+	+	+	-	+	+
ELK Packetbeat	+	+	+	+	+	+	+	+	-
NetFlow Analyzer	+	+	-	+	-	+	-	+	+

сетевого мониторинга может охватывать не весь трафик, если он не установлен в разрыв с коммутатором/свитчем. Так же такой метод при большой нагрузке на сетевое устройство может оказаться неэффективным из-за наличия слишком большого потока информации. Для аналитики сетевого трафика на уровне сеансов, используется протокол Netflow который был разработан Cisco, и де-факто является стандартом в области анализа сетевого трафика используемый большинством производителей сетевого оборудования.

Для поиска оптимального решения был проведен анализ популярных инструментов для сетевого мониторинга по следующим критериям (Таблица 1):

1. Возможность фильтрации трафика
2. Запись событий на носитель
3. Прогнозирование трендов
4. Создание отчетов SLA (Service Level Agreement)
5. Возможность оперативного оповещения о проблеме
6. Кластеризация
7. Расширенная аналитика (возможность получить доступ к телу пакета)
8. Наличие графического интерфейса
9. Аналитика flow (потока пакетов)

В качестве решения было предложено использовать сразу два подхода к мониторингу (Netflow аналитика + аналитика пакетов) сетевого трафика в связи с тем, что достоинства и недостатки обоих подходов компенсируют друг друга. Аналитику пакетов стоит применять очень избирательно, в связи с тем, что при генерации большого количества трафика, будет сгенерирован большой пласт данных, который необходимо будет обработать системе мониторинга. Netflow аналитика позволяет узнать о потоке трафике следующие параметры:

- Адрес источника
- Адрес назначения
- Порт источника для UDP и TCP
- Порт назначения для UDP и TCP
- Тип и код сообщения для ICMP
- Номер протокола IP
- Сетевой интерфейс (параметр ifindex SNMP)
- IP Type of Service

В Netflow аналитике предоставляется возможность анализа сетевого трафика на уровне сеансов, делая запись о каждой транзакции TCP/IP.

И благодаря предложению использовать комбинированный подход, будет доступна исчерпывающая информация о сетевом трафике с возможностью анализа тела пакета. Проблематика же данного подхода сводится к очень большим объемам пересылаемой информации по сети от различных источников. Поэтому, у нас должна быть возможность фильтровать трафик по определенным критериям. В качестве программных решений были выбраны следующие пакеты:

- ELK NetFlow
- ELK Packetbeat

Содержание исследования

Работа посвящена построению сетевого мониторинга, ключевой особенностью которого является возможность глубокого анализа трафика с аналитикой потока. Одной из самых важных задач является предварительное архитектурное планирование анализатора трафика с обязательным указанием необходимого функционала (для примера — какой тип трафика нам необходим, по каким портам, от каких клиентов, тип используемого протокола передачи и т.д.). От технических характеристик трафика будет зависеть, какое количество ресурсов нам необходимо для построения системы сетевого мониторинга.

В качестве основного метода исследования выбрана апробация на основании архитектуры, которая была

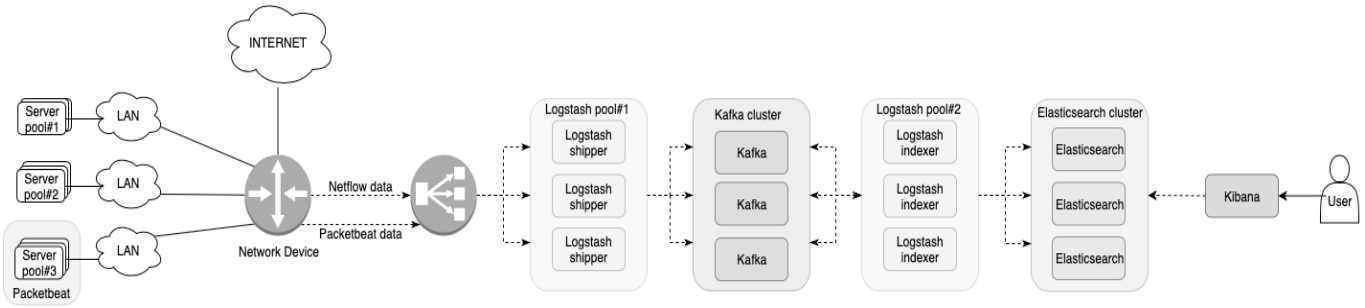

Рис. 1. Netflow Архитектура

спроектирована и введена в эксплуатацию в компании Dino Systems. В качестве экспериментального проекта был спроектирован и введен в эксплуатацию Netflow мониторинг, который на данный момент анализирует порядка 3% всего генерируемого трафика. В данном подходе не реализована расширенная аналитика пакетов. На рис. 1 показана реализация Netflow + сбор и фильтрация пакетов.

В Server pool#3 установлены агенты Packetbeat, которые считывают сетевой трафик у MySql кластера на портах 3306 и 3307 соответственно. И пересылают его через Load Balancer в Logstash pool#1 для дальнейшей пересылки в систему очередей Kafka cluster. Стоит так же отметить, что никаких других правил обработки на стороне Logstash pool#1 кроме как принятия данных на определенные порты и пересылки в систему очередей нет, соответственно задержки на этой стороне минимальны. Kafka cluster необходим для реализации системы очередей. Данное решение необходимо для того что бы иметь возможность обрабатывать эффективно волнообразную нагрузку и обеспечивать большую надежность данных, которые присылают Netflow и Packetbeat. Так же, благодаря системе очередей есть возможность создать механизм Троттлинга по определенным критериям на стороне Logstash pool#2.

На Network Device сконфигурирована работа модуля Netflow, который в свою очередь по UDP отправляет данные о каждой транзакции TCP/IP в ELK. При большой загрузке сетевого канала, Network Device будет так же нагружен из-за необходимости пересылки данных о каждой TCP/IP транзакции. Для того, чтобы частично нивелировать эту нагрузку можно воспользоваться batch-отсылкой. Фильтрация данных Packetbeat и Netflow данных возможна на стороне Logstash.

Elasticsearch — используется для хранения всех мониторинговых данных которые были отправлены сетевыми устройствами и серверами. Благодаря кластеризации, данное решение можно считать отказоустойчивым и высокодоступным. Данные Netflow и Packetbeat записываются в разные индексы (базы данных), в связи с отличающейся структурой данных. Для того, чтобы обезопасить архитектурное решение от выхода из строя одного из экземпляров приложения Elasticsearch, было указано наличие реплика-шард в мониторинговом индексе. Так же, при выходе из строя одного из экземпляров приложения, данные автоматически перебалансируются по оставшимся экземплярам приложения, и создадутся новые реплика-шарды.

Kibana используется непосредственно конечным пользователем для проведения аналитики по данным, графикам, и панель индикаторов. Так же, в Kibana доступен механизм оповещения по данным (с оповещением по email, Pagerduty, webhoock и т.д.), использование моделей машинного обучения для прогнозирования по time-series данным, обнаружение аномалий и пр. В том числе, благодаря этому инструменту есть возможность управления конфигурационными файлами Logstash прямо из UI.

Представленная система мониторинга имеет возможность масштабироваться горизонтально. Архитектурная диаграмма отображает работу только в одном дата-центра с использованием физических серверов.

Заключение

Апробация предложенного метода сетевого мониторинга успешно завершена. Была построена высокодоступная, отказоустойчивая система сетевого мониторинга с глубоким анализом сетевых данных и мониторинге потока сетевого трафика. При анализе могут применяться методы машинного обучения с помощью инструмента Kibana. Дальнейшее исследование предполагает разработку архитектуры в облаке, с использованием Kubernetes и автоматическим масштабирование системы мониторинга на основании ее загрузки, а также работу системы мониторинга cross дата-центры.

ЛИТЕРАТУРА

1. Aliev T.I., Balakshin P. V., Platunov A. E. Scientific School" Organization of Computing Systems and Networks" // Proceedings of the Thirteenth All-Russian Scientific Readings" Scientific and Technical Problems in Industry: The Future of a Strong Russia — in High Technologies" –2019.— P. 190–203
2. Kustarev P., Bykovskii S., Milin V., Antonov A. Model-driven runtime embedded monitoring for industrial controllers // 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015, Proceedings — 2015, Vol. 3, pp. 281–286
3. Shikhaliev R.G., On Methods of Monitoring Computer Networks // "Actual Problems of Information Security" III Republican Scientific and Practical Seminar, December 8, 2017, p. 38–41
4. Shikhaliev R.G., On Methods of Collecting, Storing and Analysis of Large Network Traffic // Problems of Information Technologies, 2016, No. 2, p. 56–62
5. Sultana A., Geetalaxmi J., A Review of Applications and Approaches of Network Monitoring // International Journal of Innovative Research in Computer Science & Technology, 2019, Vol.7., p.121–127.
6. Bialik M., Fadel C. Knowledge for the age of artificial intelligence: what should students learn? // Center for Curriculum Redesign. 2018. http://curriculumredesign.org/wp-content/uploads/CCR Knowledge FINAL January 2018.pdf. Last accessed 20 Oct 2019
7. Savchenko A., Vasylenko V., Kolisnyk O., Holiavkina T., Computer networks monitoring and management methods // Science-based technologies, 2018, 39.3 https://doi.org10.18372/2310–5461.39.13075
8. Hohemberger R., Lorenzon A., Rossi F., Caggiani L., Marcelo C. Optimizing Distributed Network Monitoring for NFV Service Chains // IEEE Communications Letters.2019 PP. 1–1. https://doi.org/10.1109/LCOMM.2019.2922184
9. Rahman W., Nguyen P. T., Rusliyadi M., Laxmi L., Shankar K., Network Monitoring Tools and Techniques uses in the Network Traffic Management System. International Journal of Recent Technology and Engineering.//2019 Vol.8. pp.4182–4188 https://doi.org/10.35940/ijrte.B1603.0982S1119
10. Svoboda J., Ghafir I., Prenosil V., Network Monitoring Approaches: An Overview // International Journal of Advances in Compter Networks and Its Security– IJCNS., 2015, Vol.5. pp. 88–93.

Журнал «Современная наука: актуальные проблемы теории и практики»

НИУ ИТМО