

Доклад

Мониторинг в сетях. (SNMP, агенты, Zabbix, Nagios).

Шуваев Сергей Александрович

Содержание

1	Цель работы	5
2	Задание	6
3	Доклад	7
4	Основные технологии мониторинга	8
5	Агенты мониторинга	9
6	Системы мониторинга	10
7	Nagios (и его форки: Nagios Core, Icinga, Naemon)	11
8	Prometheus + Grafana	12
9	ELK-стек (Elasticsearch, Logstash, Kibana)	13
10	Wireshark & Tcpdump	15
11	NetFlow/sFlow/IPFIX	16
12	Сравнение систем мониторинга	17
13	Рекомендации по выбору.	18
14	Источники:	19

Список иллюстраций

3.1	Общая схема	7
5.1	Simple Network Management Protocol	9
6.1	zabbix 4.0 запущенный в GNU/Linux	10
7.1	Использование Nagios	11
8.1	Использование Grafana	12
9.1	Elasticsearch	13
9.2	Как проходят данные в Logstash	14
9.3	пример отображения Kibana	14
10.1	Трафик в Wireshark	15
11.1	Оборудование в здании сети провайдера	16

Список таблиц

12.1 Таблица Сравнение систем мониторинга	17
---	----

1 Цель работы

Подготовить доклад Мониторинг в сетях. (SNMP, агенты, Zabbix, Nagios).

2 Задание

1. Темы докладов распределены по лекциям. 2. Тема должна быть уникальна в рамках направления подготовки. Дублирующие доклады не принимаются. 3. У студента учитывается только один доклад. 4. При представлении доклада после лекции, к которой привязана тема доклада, оценка снижается. 5. Оценка формируется из следующих элементов: - оформление презентации (объем презентации 5-12 слайдов); - выступление по теме доклада (5-10 минут); - содержание доклада (раскрытие темы, четкость изложения, подбор источников литературы); - оформление текста по теме доклада (5-12 стр.). - оценка выставляется только после выкладывания на сайт презентации и текста доклада. - для получения оценки обязательно представление презентации во время соответствующего лекционного занятия.

3 Доклад

Введение: Мониторинг сетевой инфраструктуры — важная задача для обеспечения стабильности, безопасности и производительности ИТ-систем. В этом отчете рассматриваются ключевые технологии и инструменты мониторинга: SNMP, агенты, Zabbix и Nagios.

Zabbix vs Nagios vs Pandora FMS(рис. 3.1).

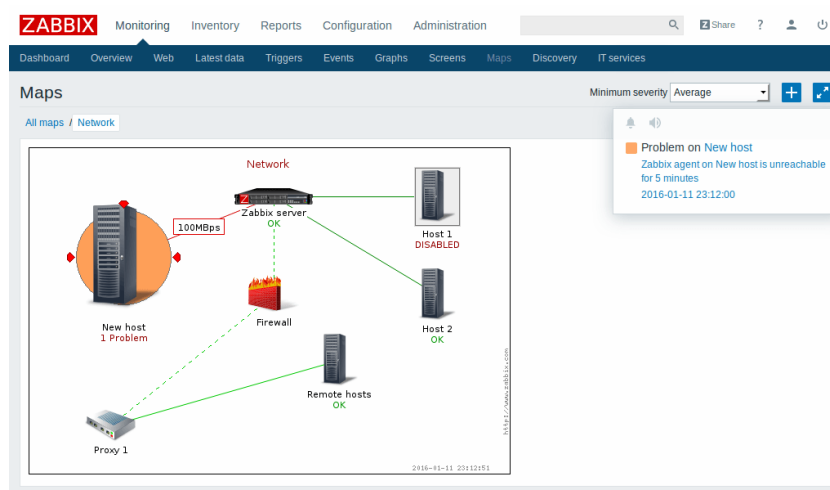


Рис. 3.1: Общая схема

4 Основные технологии мониторинга

SNMP (Simple Network Management Protocol)

Назначение: протокол для сбора и управления данными сетевых устройств (роутеры, коммутаторы, серверы).

Версии:

SNMPv1/v2c – простые, но без шифрования (используют community strings).

SNMPv3 – поддерживает аутентификацию и шифрование.

Режимы работы:

Polling – запрос данных с устройств (GET, GETNEXT).

Trap – асинхронные уведомления о событиях.

5 Агенты мониторинга

Назначение: программы, собирающие метрики с устройств и передающие их на сервер мониторинга. Типы: Встроенные (например, `snmpd` для Linux). Сторонние (Zabbix Agent, NRPE для Nagios). Преимущества: Более детальный мониторинг (диски, процессы, логи). Меньшая нагрузка на сеть по сравнению с SNMP.

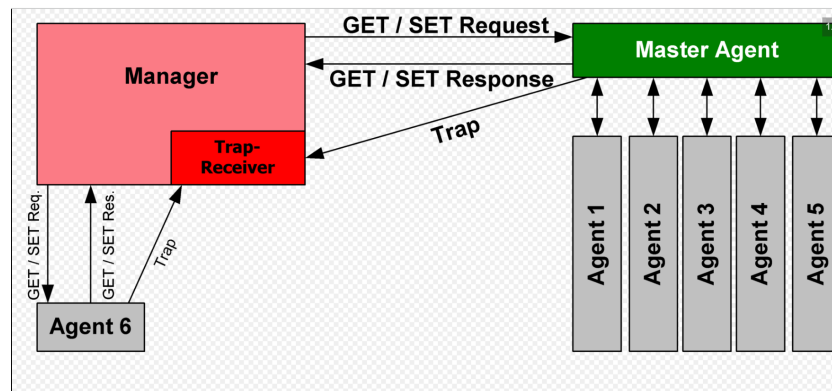


Рис. 5.1: Simple Network Management Protocol

6 Системы мониторинга

Zabbix Тип: универсальная система мониторинга с открытым исходным кодом.
Особенности: Поддержка SNMP, агентов, IPMI, JMX. Гибкие триггеры и оповещения (Email, SMS, Telegram). Встроенные шаблоны для мониторинга сетевых устройств. Визуализация через графики, дашборды, карты сетей.

Архитектура:

Сервер + агенты + веб-интерфейс + база данных (MySQL, PostgreSQL).

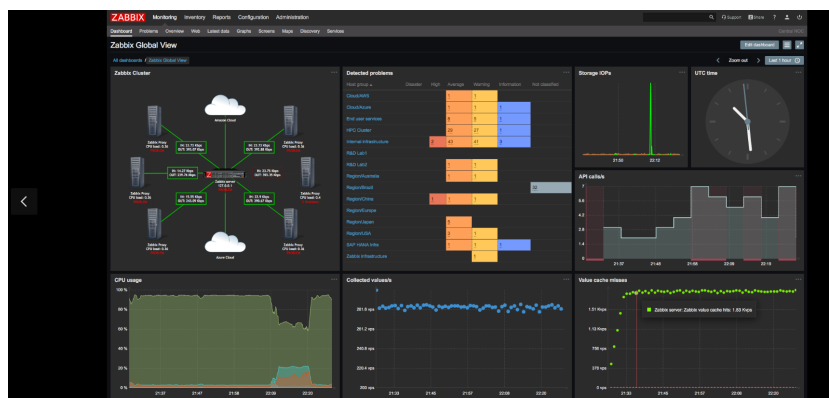


Рис. 6.1: zabbix 4.0 запущенный в GNU/Linux

7 Nagios (и его форки: Nagios Core, Icinga, Naemon)

Тип: классическая система мониторинга с упором на оповещения. Особенности: Базируется на плагинах (через NRPE или SSH). Простая конфигурация через текстовые файлы. Поддержка SNMP через дополнительные модули. Оповещения по email, SMS, мессенджерам.

Недостатки: Сложность масштабирования. Ограниченная визуализация (требуются доп. инструменты, например, Grafana).

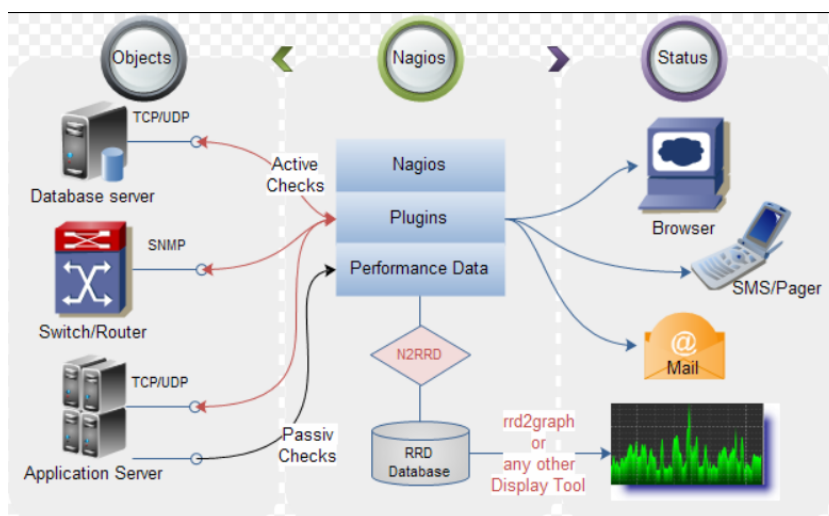


Рис. 7.1: Использование Nagios

8 Prometheus + Grafana

Тип: система мониторинга и визуализации (open-source). Особенности: Pull-модель (забирает метрики через HTTP). Многомерные данные (метки вместо иерархии). Alertmanager – управление оповещениями. Grafana – мощные дашборды.

Использование:

Мониторинг Kubernetes, микросервисов, облачных сред.

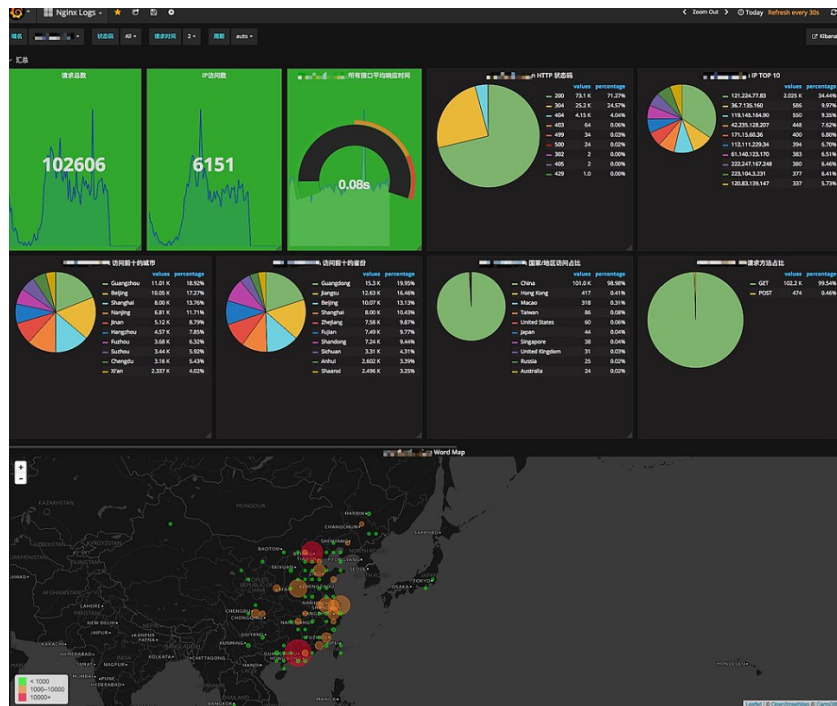


Рис. 8.1: Использование Grafana

9 ELK-стек (Elasticsearch, Logstash, Kibana)

Назначение: сбор и анализ логов. Компоненты: Filebeat – сбор логов. Logstash – обработка и фильтрация. Elasticsearch – хранение и поиск. Kibana – визуализация.

Применение:

Анализ сетевых аномалий, безопасность (SIEM).

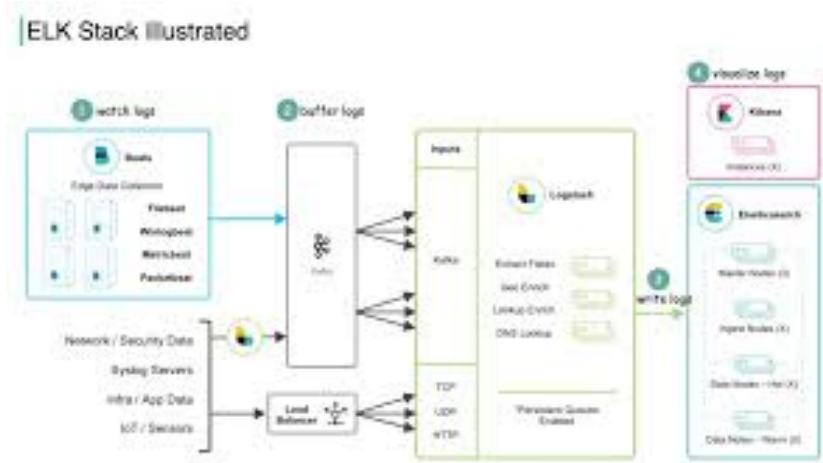


Рис. 9.1: Elasticsearch



Рис. 9.2: Как проходят данные в Logstash

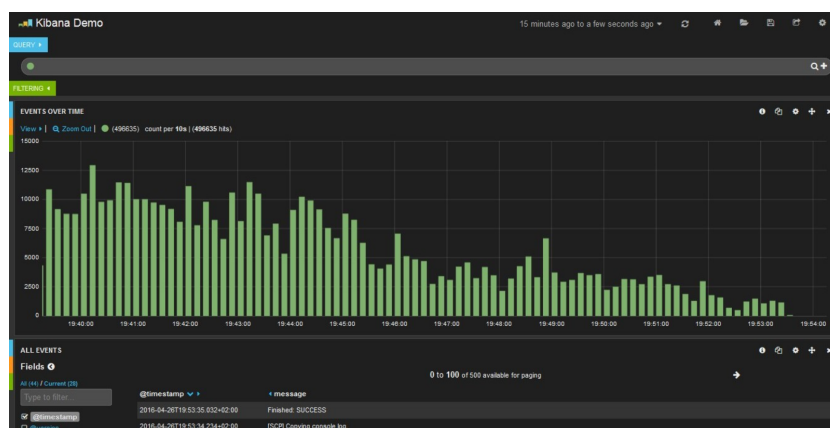
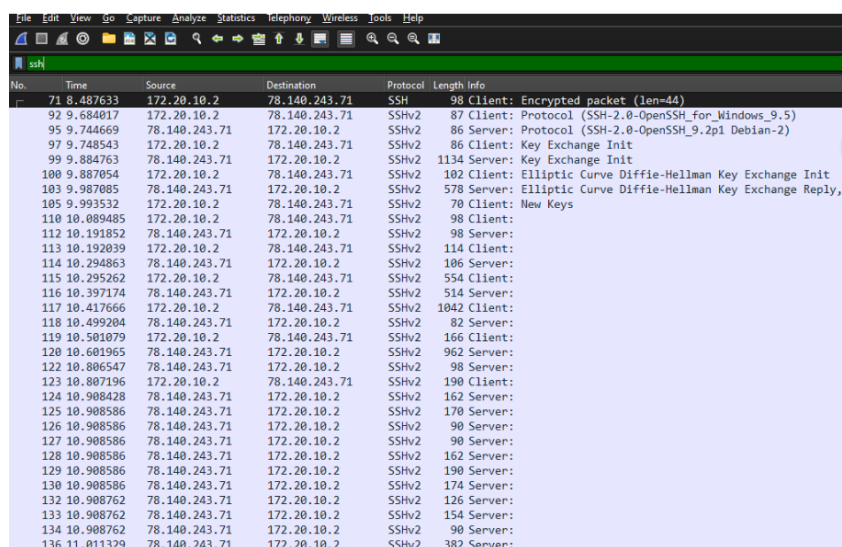


Рис. 9.3: пример отображения Kibana

10 Wireshark & Tcpdump

Назначение: глубокий анализ сетевого трафика. Использование: Диагностика DDoS, атак, проблем с QoS. Фильтрация по IP, портам, протоколам.



No.	Time	Source	Destination	Protocol	Length	Info
71	8.487633	172.20.10.2	78.140.243.71	SSH	98	Client: Encrypted packet (len=44)
92	9.684017	172.20.10.2	78.140.243.71	SSHv2	87	Client: Protocol (SSH-2.0-OpenSSH_for_Windows_9.5)
95	9.744669	78.140.243.71	172.20.10.2	SSHv2	86	Server: Protocol (SSH-2.0-OpenSSH_9.2p1 Debian-2)
97	9.748543	172.20.10.2	78.140.243.71	SSHv2	86	Client: Key Exchange Init
99	9.884763	78.140.243.71	172.20.10.2	SSHv2	1134	Server: Key Exchange Init
100	9.887054	172.20.10.2	78.140.243.71	SSHv2	102	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
103	9.987085	78.140.243.71	172.20.10.2	SSHv2	578	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply
105	9.993532	172.20.10.2	78.140.243.71	SSHv2	70	Client: New Keys
110	10.089485	172.20.10.2	78.140.243.71	SSHv2	98	Client:
112	10.191852	78.140.243.71	172.20.10.2	SSHv2	98	Server:
113	10.192039	172.20.10.2	78.140.243.71	SSHv2	114	Client:
114	10.294863	78.140.243.71	172.20.10.2	SSHv2	106	Server:
115	10.295262	172.20.10.2	78.140.243.71	SSHv2	554	Client:
116	10.397174	78.140.243.71	172.20.10.2	SSHv2	514	Server:
117	10.417666	172.20.10.2	78.140.243.71	SSHv2	1042	Client:
118	10.499204	78.140.243.71	172.20.10.2	SSHv2	82	Server:
119	10.501079	172.20.10.2	78.140.243.71	SSHv2	166	Client:
120	10.601965	78.140.243.71	172.20.10.2	SSHv2	962	Server:
122	10.806547	78.140.243.71	172.20.10.2	SSHv2	98	Server:
123	10.807196	172.20.10.2	78.140.243.71	SSHv2	190	Client:
124	10.908428	78.140.243.71	172.20.10.2	SSHv2	162	Server:
125	10.908586	78.140.243.71	172.20.10.2	SSHv2	170	Server:
126	10.908586	78.140.243.71	172.20.10.2	SSHv2	90	Server:
127	10.908586	78.140.243.71	172.20.10.2	SSHv2	90	Server:
128	10.908586	78.140.243.71	172.20.10.2	SSHv2	162	Server:
129	10.908586	78.140.243.71	172.20.10.2	SSHv2	190	Server:
130	10.908586	78.140.243.71	172.20.10.2	SSHv2	174	Server:
132	10.908762	78.140.243.71	172.20.10.2	SSHv2	126	Server:
133	10.908762	78.140.243.71	172.20.10.2	SSHv2	154	Server:
134	10.908762	78.140.243.71	172.20.10.2	SSHv2	90	Server:
136	11.011329	78.140.243.71	172.20.10.2	SSHv2	382	Server:

Рис. 10.1: Трафик в Wireshark

11 NetFlow/sFlow/IPFIX

Назначение: мониторинг трафика (источник/получатель, объемы). Инструменты: nProbe, ntopng, SolarWinds NetFlow Traffic Analyzer.(рис. 11.1)

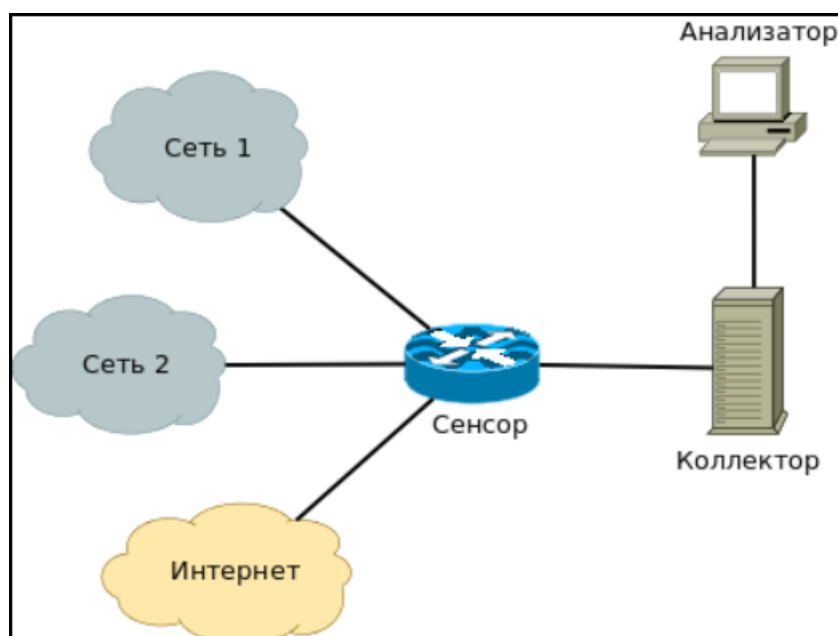


Рис. 11.1: Оборудование в здании сети провайдера

12 Сравнение систем мониторинга

Таблица 12.1: Таблица Сравнение систем мониторинга

Крите- рий	Zabbix	Nagios	Prometheus	ELK
Тип данных	Метрики + логи (с дополнениями)	Метрики (через плагины)	Метрики + события	Логи + трафик
Мас- штаби- руе- мость	Высокая (Прогу, кластеризация)	Средняя (требуется доп. настроек)	Очень высокая (для cloud-native)	Высокая (шар- дирование в ES)
Визуа- лиза- ция	Дашборды, графики, карты	Ограниченная (нужна Grafana)	Grafana	Kibana (лог- аналитика)
Опове- щения	Гибкие (Email, SMS, Telegram)	Email, SMS, скрипты	Alertmanager (Slack, PagerDuty)	Watchers (алерты на логи)
Слож- ность	Средняя	Низкая (базовый функционал)	Высокая (требуется понимания метрик)	Высокая (настройка pipelines)

13 Рекомендации по выбору.

Для сетевого оборудования ☒ Zabbix + SNMP. Для облаков и микросервисов ☒ Prometheus + Grafana. Для логов и безопасности ☒ ELK-стек. Для глубокого анализа трафика ☒ Wireshark + NetFlow.

14 Источники:

По SNMP и сетевому мониторингу:

Mauro, D., Schmidt, K. Essential SNMP (2nd Edition). O'Reilly, 2005.

Habraken, J. Network Monitoring & Management. Cisco Press, 2006.

По Zabbix и Nagios:

Liebling, A. Zabbix 6 IT Infrastructure Monitoring Cookbook. Packt, 2022.

Barth, W. Nagios: System and Network Monitoring (2nd Ed.). No Starch Press, 2008.

По Prometheus и Grafana:

Jablonski, J. Prometheus: Up & Running (2nd Ed.). O'Reilly, 2023.

Smith, M. Grafana Dashboards for Monitoring. Apress, 2021.

По ELK и анализу логов:

Gheorghe, A. Elasticsearch 8 in Action. Manning, 2023.

Gururajan, P. Learning ELK Stack (2nd Ed.). Packt, 2017.