

Доклад

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

Шуваев С. А.

Российский университет дружбы народов, Москва, Россия

Информация

- Шуваев Сергей Александрович
- студент
- Российский университет дружбы народов
- 1032224269@pfur.ru
- <https://Grinders060050.github.io/ru/>



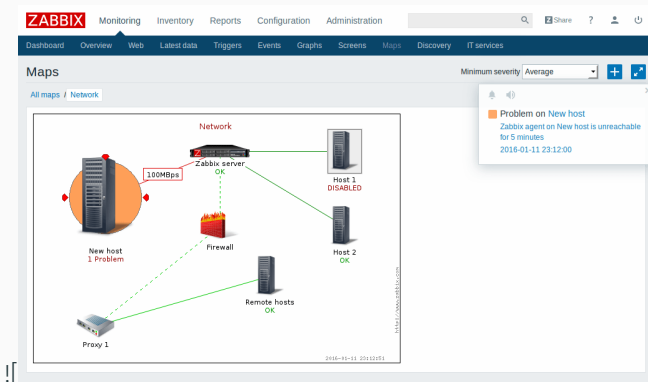
Figure 1: Студент 3 курса.

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

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

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

“Zabbix vs Nagios vs Pandora FMS”



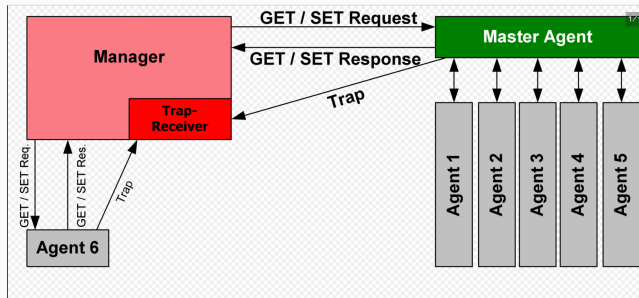


Figure 2: Simple Network Management Protocol

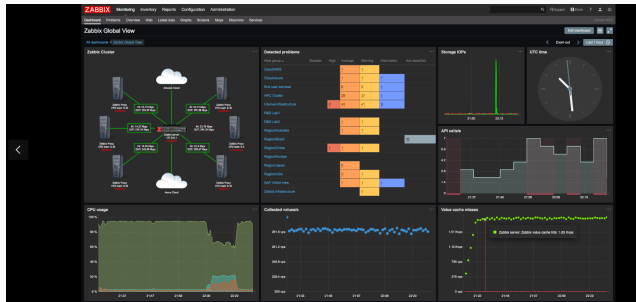


Figure 3: zabbix 4.0 запущенный в GNU/Linux

“Nagios (и его форки: Nagios Core, Icinga, Naemon)”

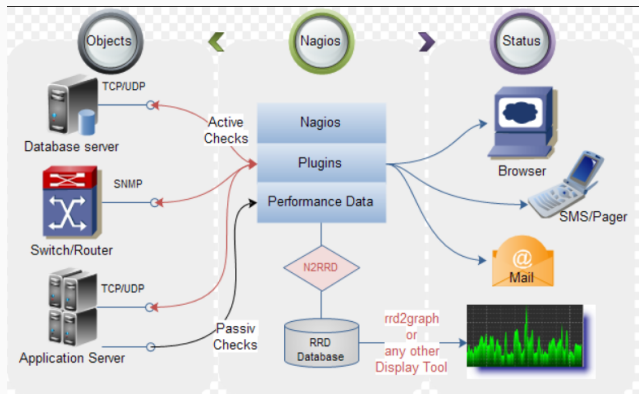


Figure 4: Использование Nagios

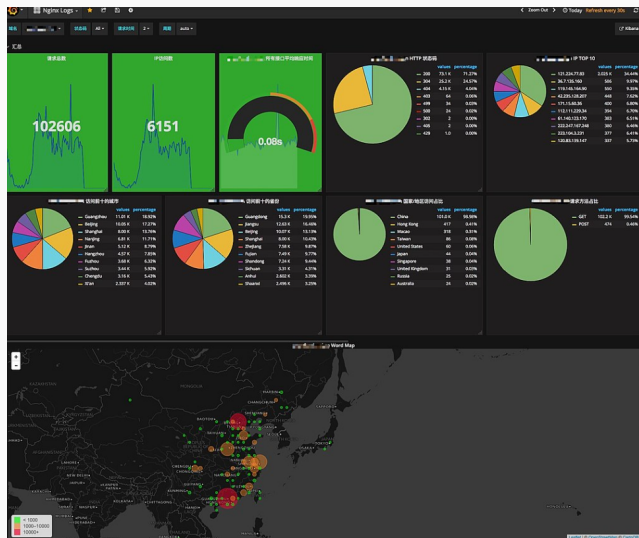


Figure 5: Использование Grafana

ELK-стек (Elasticsearch, Logstash, Kibana)

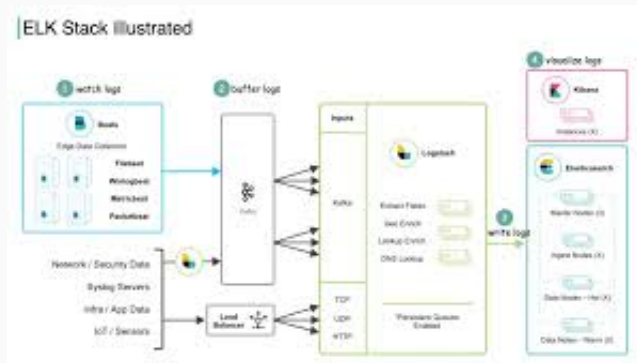


Figure 6: Elasticsearch



Figure 7: Как проходят данные в Logstash

ELK-стек (Elasticsearch, Logstash, Kibana)

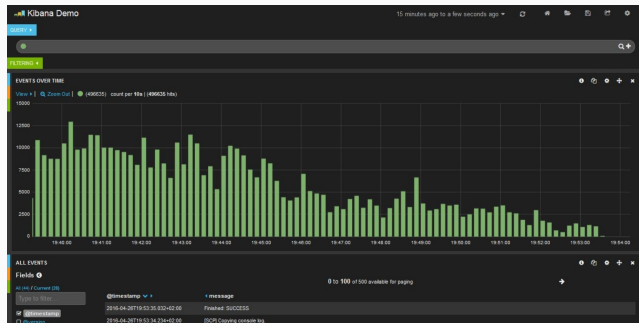
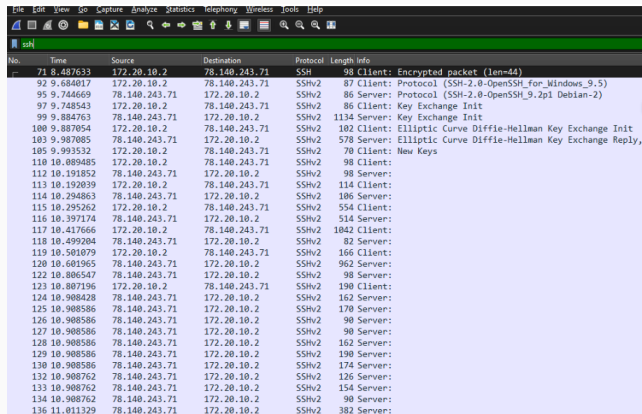


Figure 8: пример отображения Kibana

Wireshark & Tcpdump



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:

Figure 9: Трафик в Wireshark

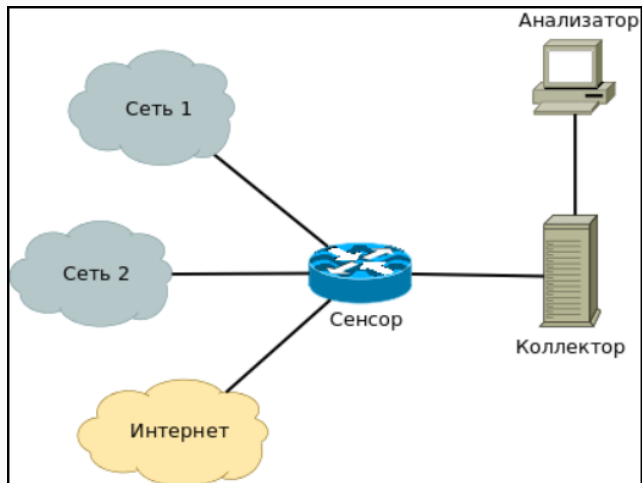


Figure 10: Оборудование в здании сети провайдера

Table 1: Таблица Сравнение систем мониторинга

Крите- рий	Zabbix	Nagios	Prometheus	ELK
Тип данных	Метрики + логи (с дополнениями)	Метрики (через плагины)	Метрики + события	Логи + трафик
Масшта- бируе- мость	Высокая (Proxu, кластеризация)	Средняя (требует доп. настроек)	Очень высокая (для cloud-native)	Высокая (шардирование в ES)
Визуали- зация	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-	Средняя	Низкая (базовый	Высокая (требует	Высокая

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