

Мониторинг и логирование: Zabbix, Prometheus, ELK

Практикум по мониторингу и логированию, как инфраструктуры так и приложений с помощью Zabbix, Prometheus, Grafana и ELK

Длительность курса: 78 академических часов

1 Мониторинг и алертинг

- Задачи мониторинга и алертинга**
 - разобраться в том, что такое мониторинг;
 - объяснить как строить мониторинг правильно;
 - рассмотреть хорошие и плохие паттерны мониторинга.

Black/white boxing
инструменты мониторинга
инструменты алертинга
time-series базы данных

- Netdata**

- 1 Установка и конфигурация**

рассмотреть варианты установки Zabbix.

использование различных СУБД для хранения метрик;
установка на ОС;
использование mysql, postgres, etc.

- 2 Discovery Trapper**

рассмотреть отсылку данных в zabbix без использования агентов.

- 3 Мониторинг порталов и баз данных**

Рассмотреть подходы к мониторингу доступности веб-порталов и их основных компонентов

- 4 Графики и комплексные экраны**

сформировать комплексные экраны для отображения данных мониторинга, дашбордов и графиков;
настроить разрешения, добавления элементов, формирование комплексных экранов.

- 5 Настройка алертинга**

рассмотреть подходы к отправке уведомлений;
рассмотреть каналы доставки уведомлений.

почта, смс, телеграмм, etc.

Домашние задания

- 1** Настройка zabbix, создание LLD, оповещение на основе триггеров

Цель: Установить и настроить zabbix, настроить автоматическую отправку алертов в телеграмм канал

Домашнее задание представляет из себя следующее.

Необходимо сформировать скрипт генерирующий метрики формата:

```
otus_important_metrics[metric1]
otus_important_metrics[metric2]
otus_important_metrics[metric3]
```

С рандомным значение от 0 до 100

Создать правила LLD для обнаружения этих метрик и автоматического добавления триггеров. Триггер должен срабатывать тогда когда значение больше или равно 95.

Реализовать автоматическую отправку уведомлений в телеграмм канал.

В качестве результаты выполнения дз Вы должны предоставить скрипт генерации метрик, скриншоты

графиков полученных метрик, ссылку на телеграмм канал с уже отправленными уведомлениями.

1 Prometheus как новый виток систем мониторинга

рассмотреть историю развития проекта, архитектуры, возможности, примеры использования.

2 Prometheus экспортеры

рассмотреть основные возможности экспортеров.

экспортеры и для чего они нужны, мониторинг инстансов, СУБД, веб серверов, серверов сообщений, etc; exporters, db exporters, node exporter, etc.

Домашние задания

1 Установка и настройка Prometheus, использование exporters

Цель: Необходимо собрать стенд включающий в себя 2 виртуальные машины:

1. Prometheus
2. Nginx

На вм с nginx установить и настроить nginx-exporter.

С помощью siege (или apache benchmark, или yandex tank) устроить ипровизированное нагрузочное тестирование.

Посчитать 99й перцентиль по времени ответа за 5 минут.

Посчитать количество запросов по каждому коду ответа за 5 минут.

Реализовать свой собственный экспортер с собственными метриками (ваше имя\никнейм в название метрики) используя любой ЯП. (Ссылка с реализацией экспортера на bash прилагается)

Для сдачи:

1. Скриншоты с prometheus с результатами запросов PromQL
 2. Текстовый файл с примерами метрик вашего экспортера
-

3 Prometheus Alerting

объяснить различные пути отправки уведомлений.

формирование уведомлений, отправка в различные каналы: почта, слак, телерамм, смс.

- 1 **Grafana как универсальный инструмент визуализации**

рассмотреть построение графиков из различных источников данных при помощи Grafana.

история проекта, использование различных источников, хранилище дашбордов, формирование и версионирование собственных дашбордов.

- 2 **Grafana формирование дашбордов**

проанализировать возможности по формирования дашбордов.

использование дашбордов, тиражирование, использование переменных, формирование дашбордов для различных окружений.

Домашние задания

 - 1 Формирование dashboard на основе собранных данных с Prometheus

использовать графану zabbix.systemctl.su
создать своего пользователя
создать свой team
разрешить доступ к своей дашборде только своей team
подключить свой прометеус со своим экспортером к графани
создать свою папку
создать свой дашбоард на основе метрик со своего экспортера
настроить threshold
настроить alert в телеграм канал (указан в ДЗ про алертинг с заббикса)
сделать снэпшот

Как результат ДЗ прислать ссылку на снэпшот, ссылку на дашборду
по просьбе преподавателя уметь пересоздать дашборду из сохраненного json

- 1 **Классическое логирование в Linux**

Понять зачем нужны логи и как их собирать
Освоить принципы логирования с помощью rsyslog
Понять возможности logrotate для задач ротации логов
Научиться работать с journald и auditd
Узнать про adrttd и kdump

- 2 **Системы логирования (ELK, EFK, Graylog2)**

сравнить различные системы логирования, присутствующих на рынке.

история систем, обзор ELK, EFK - fluentd, Graylog2.

- 3 **ELK стэк**

рассмотреть ELK стек.

Elasticsearch, Logstash, Kibana

Домашние задания

 - 1 Установка ELK

Цель: Для успешного выполнения ДЗ вам необходимо установить ELK (elasticsearch, logstash, kibana).
Базовая операционная система - по вашему выбору.
После успешной установки ELK-стека вам необходимо настроить отправку логов sshd в elasticsearch через logstash.
Для этого вам придется изменить настройку rsyslog.
Проверьте созданся ли index в elasticsearch.
После настройки отправки логов в ELK попробуйте настроить визуализацию логов от sshd в kibana.
В качестве результата ДЗ принимается: конфиг rsyslog, конфиг logstash и результат проверки index в elasticsearch, а также скриншот из kibana, если получилось настроить визуализацию.

- 4 **Logstash**

- 5 **Hearthbeat, metricbeat, filebeat, fluentbit**

Проанализировать особенности beats-агентов для стека ELK.
Рассмотреть конфигурации различных агентов, получение данных, формирование аналитической информации.

Домашние задания

 - 1 Установка beats

Цель: Для успешного выполнения дз вам нужно сконфигурировать hearthbeat, filebeat и metricbeat.

Heartbeat должен проверять доступность следующих ресурсов: otus.ru, google.com.

Metricbeat должен формировать метрики на основе показателей загрузки процессора и оперативной памяти.

Filebeat должен собирать логи ssh сервера. По собственному усмотрению вы можете собирать логи других сервисов которые присутствуют в системе ^_^

В качестве результата приложите конфиги hearthbeat, filebeat и metricbeat. Скриншот полученных данных отображенных в Kibana.

6 Apache Kafka в логировании

7 Kibana как инструмент визуализации логов

проанализировать особенности визуализации данных в Kibana.
история проекта, формирование дашбордов.

1 Консультация по итоговому проекту

2 Итоговый проект

защитить проект и получить рекомендации экспертов.

Домашние задания

1 Итоговый проект

Цель: В курсовом проекте вам предстоит развернуть заранее созданную инфраструктуру при помощи Vagrant и Ansible. И настроить полный цикл мониторинга и логирования.

Инфраструктура включает в себя: ОС Ubuntu 18.04, Postgresql 11 (petroni cluster), consul (cluster, template, agent), nginx, pgbouncer, wordpress site.