OTUS

ОНЛАЙН-ОБРАЗОВАНИЕ

Онлайн-образование

Меня хорошо видно && слышно?

Ставьте плюсы, если все хорошо

Напишите в чат, если есть проблемы

Правила вебинара

- Активно участвуем
- Задаем вопросы в чат или голосом
- Off-topic обсуждаем в Slack #канал группы или #general
- Вопросы вижу в чате, могу ответить не сразу

Beats: Data shippers

Маршрут вебинара

- Beats: Data shippers
- Heartbeat
- Auditbeat
- Metricbeat
- Filebeat
- Fluentbit

Цели занятия

После занятия вы сможете:

1. Понять основные принципы работы поставщиков данных стека ELK
2. Установить и настроить поставщики данных
3. Освоить базовые навыки анализа данных

Смысл

Зачем вам это уметь:

1. Чтобы понимать основные особенности использования различных поставщиков данных
2. Чтобы наиболее эффективно использовать изученные элементы для сбора информации в вашей инфраструктуре

Beats: Data shippers

Beats: Data shippers

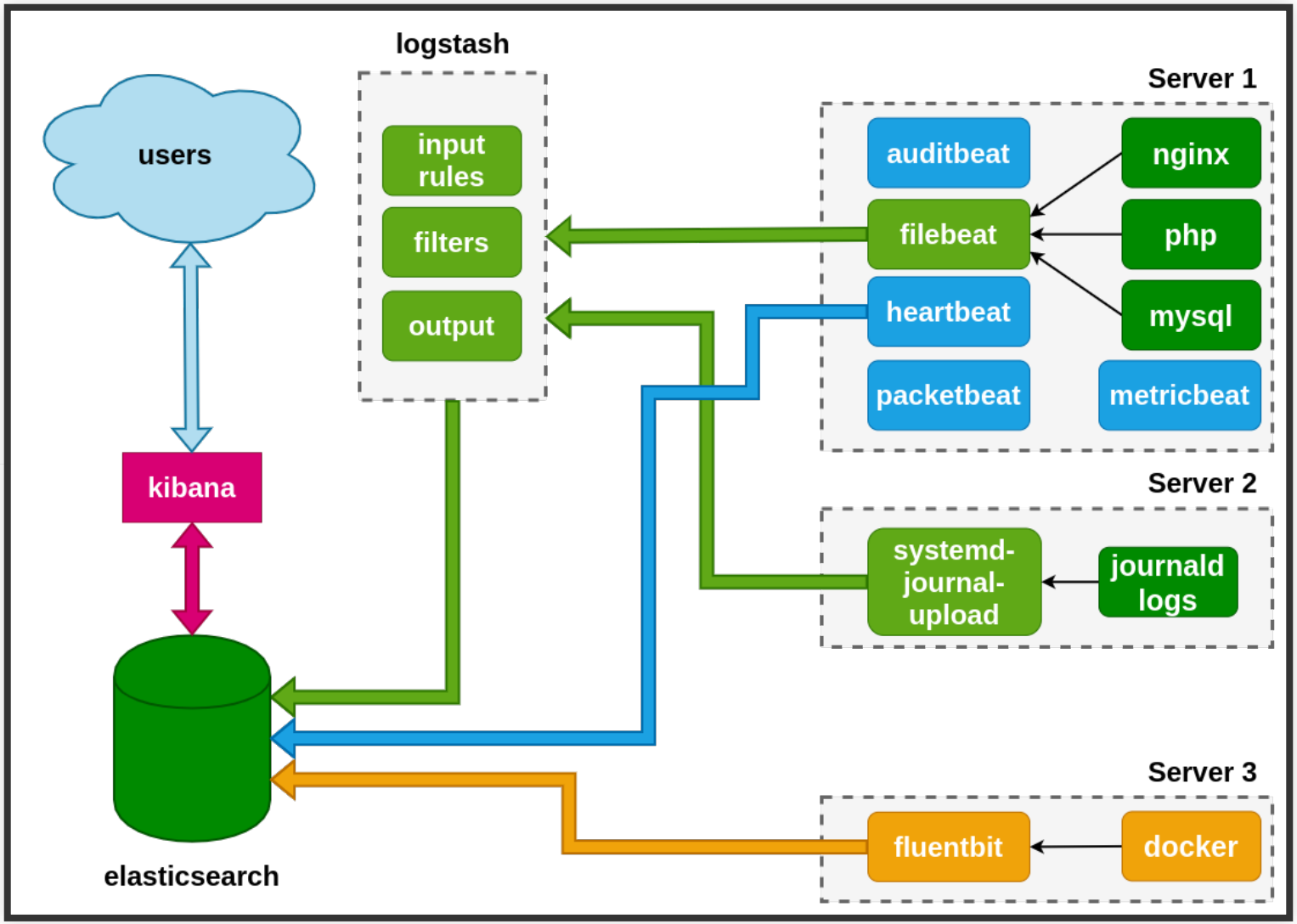
Beats - это поставщики данных для обработки в стеке ELK

Основные поставщики:

- Filebeat
- Metricbeat
- Packetbeat
- Winlogbeat
- Auditbeat
- Heartbeat
- Functionbeat

https://www.elastic.co/beats/

Beats: Data shippers



Маршрут вебинара

- Beats: Data shippers
- Heartbeat
- Auditbeat
- Metricbeat
- Filebeat
- Fluentbit

Heartbeat

Heartbeat

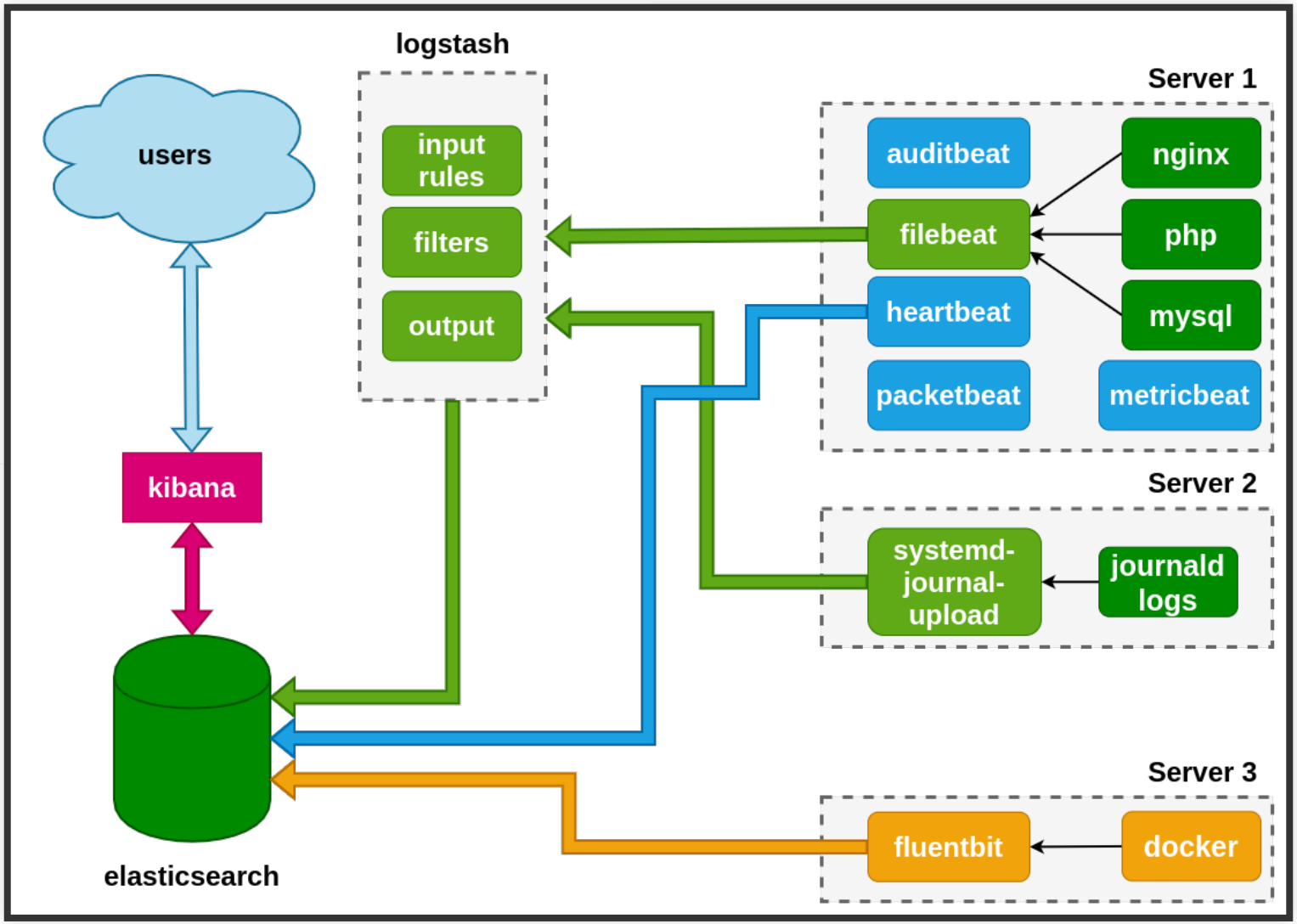
Heartbeat

Heartbeat - устанавливается на удаленный сервер и проводит периодические проверки сервисов

Особенности:

- Умеет пинговать по ICMP, TCP и HTTP
- Поддерживает TLS, аутентификацию и прокси
- Может мониторить не только внутренние, но и внешние ресурсы
- Поддерживает возможность вывода в Logstash или в базу Elasticsearch

Heartbeat


logstash
input rules
filters
output
users
kibana
elasticsearch
Server 1
auditbeat
filebeat
heartbeat
packetbeat
nginx
php
mysql
metricbeat
Server 2
systemd-journal-upload
journald logs
Server 3
fluentbit
docker

Установка heartbeat

Добавляем ключ репозитория:

```
rpm --import https://packages.elastic.co/GPG-KEY-elasticsearch
```

Добавляем репозиторий:

```
cat /etc/yum.repos.d/elastic.repo
[elastic-7.x]
name=Elastic repository for 7.x packages
baseurl=https://artifacts.elastic.co/packages/7.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
```

Установка heartbeat

Устанавливаем heartbeat:

```
yum install -y heartbeat-elastic
```

Пример конфигурации heartbeat:

```
cat /etc/heartbeat/heartbeat.yml
heartbeat.config.monitors:
  path: ${path.config}/monitors.d/*.yml
  reload.enabled: false
  reload.period: 5s
- type: http
  urls: ["http://localhost:9200"]
  schedule: '@every 10s'
```

Пример конфигурации heartbeat

Конфигурация шаблонов и интерфейса Kibana:

```
setup.template.settings:
  index.number_of_shards: 1
  index.codec: best_compression
setup.kibana:
  host: "localhost:5601"
```

Пример конфигурации heartbeat

Конфигурация вывода и передачи сообщений:

```
#output.elasticsearch:
#  hosts: ["localhost:9200"]

  #protocol: "https"
  #username: "elastic"
  #password: "changeme"

output.logstash:
  hosts: ["logstash_host:5044"]
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]
  #ssl.certificate: "/etc/pki/client/cert.pem"
  #ssl.key: "/etc/pki/client/cert.key"
```

Проверка конфигурации heartbeat:

```
heartbeat test config
```

Ваши вопросы?

Маршрут вебинара

- Beats: Data shippers
- Heartbeat
- Auditbeat
- Metricbeat
- Filebeat
- Fluentbit

Auditbeat

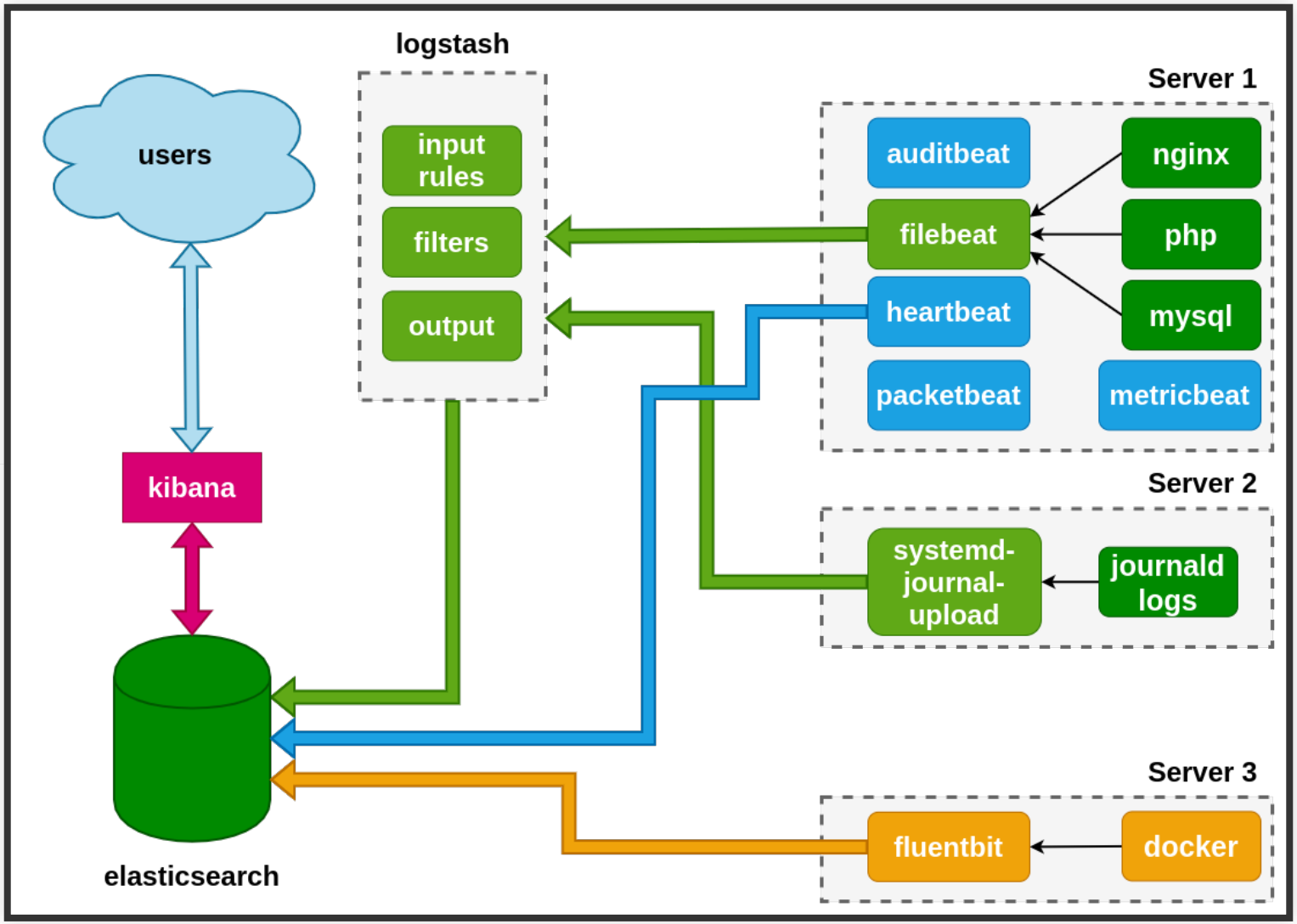
Auditbeat

Auditbeat - собирает и передает события публикуемые Linux Audit Framework (auditd)

Особенности:

- Сбор событий безопасности сервера
- Сбор любых кастомных событий сервера
- Поддерживает возможность вывода в Logstash или в базу Elasticsearch

Auditbeat


logstash
input rules
filters
output
users
kibana
elasticsearch
Server 1
auditbeat
filebeat
heartbeat
packetbeat
nginx
php
mysql
metricbeat
Server 2
systemd-journal-upload
journald logs
Server 3
fluentbit
docker

Установка auditbeat

Устанавливаем auditbeat:

```
yum install -y auditbeat
```

Пример конфигурации auditbeat:

```
cat /etc/auditbeat/auditbeat.yml
auditbeat.modules:
- module: auditd
  audit_rule_files: [ '${path.config}/audit.rules.d/*.conf' ]
  audit_rules: |

- module: file_integrity
  paths:
  - /bin
  - /usr/bin
  - /sbin
  - /usr/sbin
  - /etc
```

Установка auditbeat

Пример конфигурации auditbeat:

```
- module: system
  datasets:
    - host    # General host information, e.g. uptime, IPs
    - login   # User logins, logouts, and system boots.
    - package # Installed, updated, and removed packages
    - process # Started and stopped processes
    - socket  # Opened and closed sockets
    - user    # User information
```

Установка auditbeat

Пример конфигурации auditbeat:

```
# How often datasets send state updates with the
# current state of the system (e.g. all currently
# running processes, all open sockets).
state.period: 12h

# Enabled by default. Auditbeat will read password fields in
# /etc/passwd and /etc/shadow and store a hash locally to
# detect any changes.
user.detect_password_changes: true

# File patterns of the login record files.
login.wtmp_file_pattern: /var/log/wtmp*
login.btmp_file_pattern: /var/log/btmp*
```

Ваши вопросы?

Маршрут вебинара

- Beats: Data shippers
- Heartbeat
- Auditbeat
- Metricbeat
- Filebeat
- Fluentbit

Metricbeat

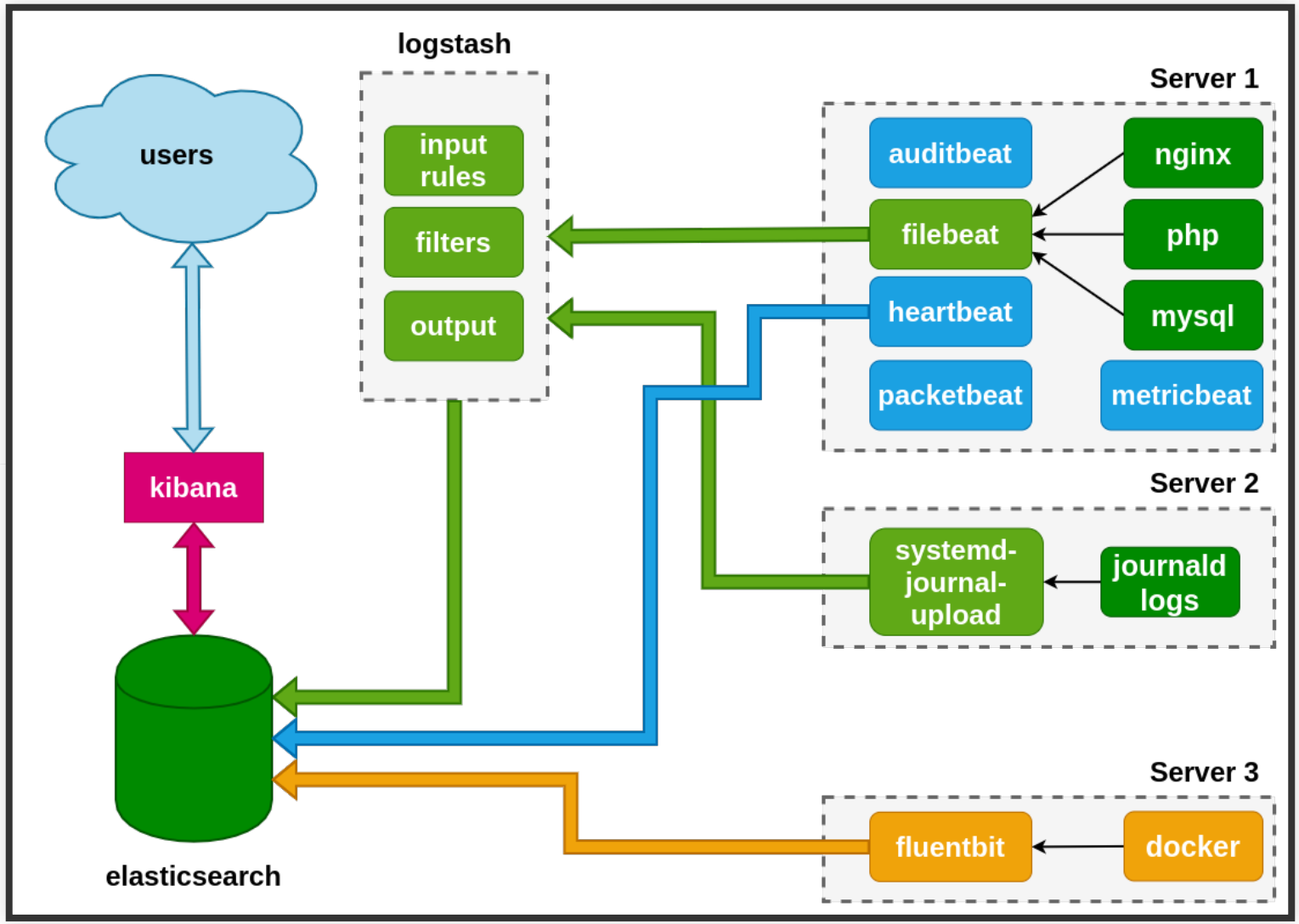
Metricbeat

Metricbeat - собирает и передает метрики с сервера и сервисов, которые запущены на этом сервере

Особенности:

- Сбор метрик по подсистемам сервера (CPU, память, диски, сеть)
- Сбор метрик распространенных сервисов (apache, nginx, mysql, docker, kubernetes)
- Поддерживает возможность вывода в Logstash или в базу Elasticsearch

Metricbeat


logstash
input rules
filters
output
users
kibana
elasticsearch
Server 1
auditbeat
filebeat
heartbeat
packetbeat
nginx
php
mysql
metricbeat
Server 2
systemd-journal-upload
journald logs
Server 3
fluentbit
docker

Установка metricbeat

Устанавливаем metricbeat:

```
yum install -y metricbeat
```

Пример конфигурации metricbeat:

```
cat /etc/metricbeat/metricbeat.yml
metricbeat.config.modules:
  # Glob pattern for configuration loading
  path: ${path.config}/modules.d/*.yml

  # Set to true to enable config reloading
  reload.enabled: false

  # Period on which files under path should be checked for ...
  #reload.period: 10s
```

Установка metricbeat

Пример конфигурации metricbeat:

```
setup.template.settings:
  index.number_of_shards: 1
  index.codec: best_compression

setup.kibana:
  host: "elk-lab-main:5601"

output.elasticsearch:
  hosts: ["elk-lab-main:9200"]
```

Установка metricbeat

Включение модулей metricbeat nginx и mysql:

```
cd /etc/metricbeat/modules.d/
mv nginx.yml.disabled nginx.yml
mv mysql.yml.disabled mysql.yml
```

Для nginx: не забыть настроить stub location

Для mysql: настроить доступ в базу пользователю

Ваши вопросы?

Маршрут вебинара

- Beats: Data shippers
- Heartbeat
- Auditbeat
- Metricbeat
- Filebeat
- Fluentbit

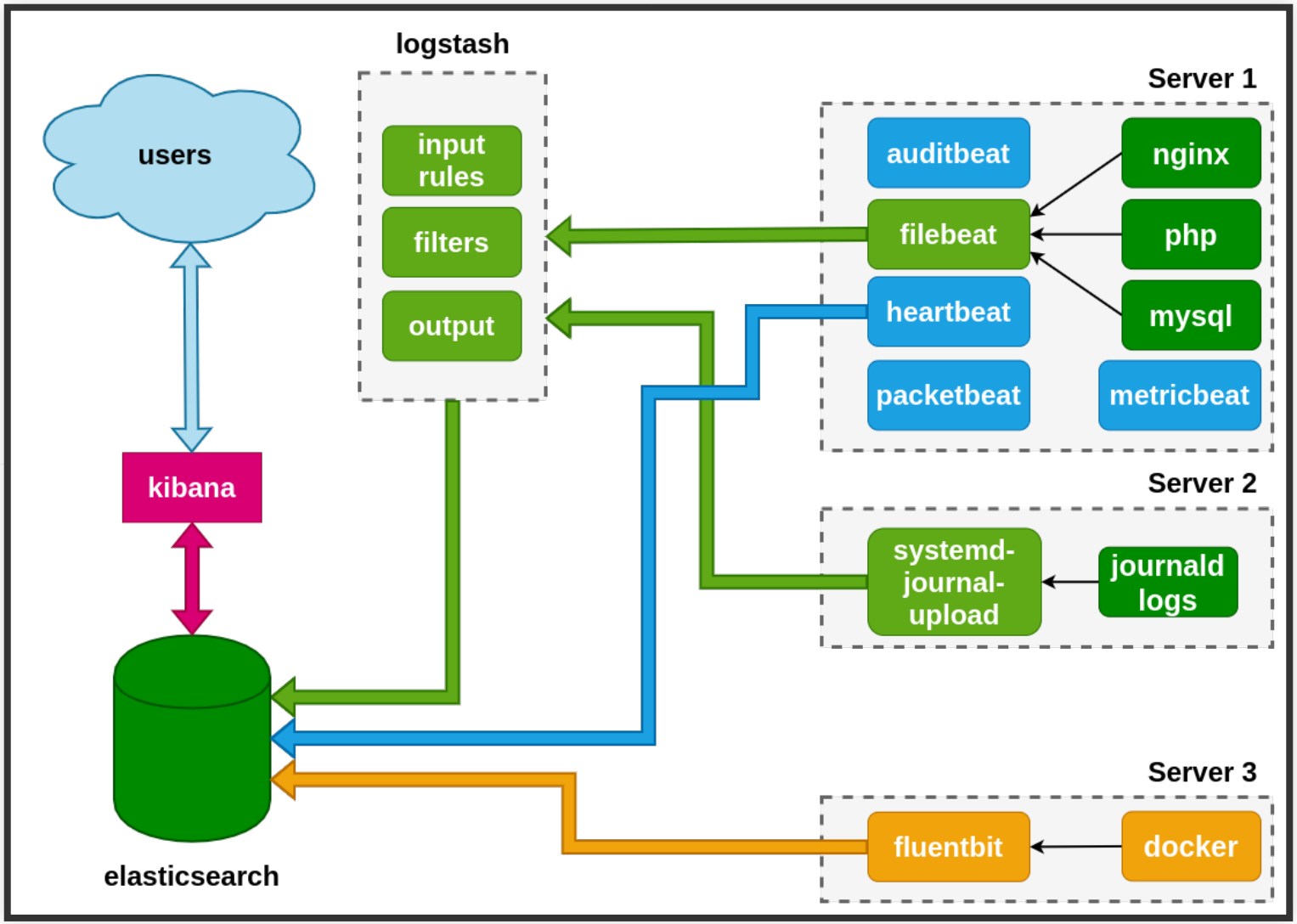
Filebeat

Filebeat - основной поставщик данных в ELK

Особенности:

- Большое количество вариантов ввода данных (files, syslog, stdin, docker, json, MQTT, netflow)
- Возможность базовой фильтрации и модификации сообщений
- Возможность вывода в Logstash или в базу Elasticsearch напрямую

Filebeat


logstash
input rules
filters
output
users
kibana
elasticsearch
Server 1
auditbeat
filebeat
heartbeat
packetbeat
nginx
php
mysql
metricbeat
Server 2
systemd-journal-upload
journald logs
Server 3
fluentbit
docker

Установка filebeat

Устанавливаем filebeat:

```
yum install -y filebeat
```

Пример конфигурации filebeat:

```
cat /etc/filebeat/filebeat.yml
- type: log
  enabled: true
  paths:
      - /var/log/nginx/access.log
  fields:
    service: nginx_access
  fields_under_root: true
  scan_frequency: 5s
```

Пример конфигурации filebeat

Конфигурация модулей и шаблонов:

```
filebeat.config.modules:
  # Glob pattern for configuration loading
  path: ${path.config}/modules.d/*.yml

  # Set to true to enable config reloading
  reload.enabled: false

setup.template.settings:
  index.number_of_shards: 3
```

Пример конфигурации filebeat

Конфигурация вывода и передачи сообщений:

```
#output.elasticsearch:
#  hosts: ["localhost:9200"]

  #protocol: "https"
  #username: "elastic"
  #password: "changeme"

output.logstash:
  hosts: ["logstash_host:5044"]
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]
  #ssl.certificate: "/etc/pki/client/cert.pem"
  #ssl.key: "/etc/pki/client/cert.key"
```

Проверка конфигурации filebeat:

```
filebeat test config
```

Пример конфигурации filebeat

Настройка multiline:

```
multiline.pattern: ^\[
multiline.negate: false
multiline.match: before
```

multiline.pattern: ^[- описывает регулярное выражение, на которое будет срабатывать правило (в логах это начало строки с timestamp)

multiline.negate: false - инвертирование результата

multiline.match: before - условие присоединения найденной строки к следующей

Пример конфигурации filebeat

Пример токенизации входящих строк с использованием пользовательского паттерна:

```
processors:
  - dissect:
      tokenizer: "%{key1} %{key2} %{key3|convert_datatype}"
      field: "message"
      target_prefix: "dissect"
```

https://www.elastic.co/guide/en/beats/filebeat/master/dissect.html

Пример конфигурации filebeat

Конфигурация для обработки логов docker (файлы и json):

```
filebeat.inputs:
- type: container
  paths:
    - /var/lib/docker/containers/*/*.log
- type: docker
  containers.ids:
  - "*"
  processors:
  - add_kubernetes_metadata:
  - drop_event:
      when:
        equals:
          kubernetes.container.name: "filebeat"
```

Пример конфигурации filebeat

Конфигурация для обработки логов docker (stream):

```
filebeat.inputs:
- type: docker
  combine_partial: true
  containers:
    path: "/var/lib/docker/containers"
    stream: "stdout"
    ids:
      - "*"
  processors:
  - add_kubernetes_metadata:
  - drop_event:
      when:
        equals:
          kubernetes.container.name: "filebeat"
```

Пример конфигурации filebeat

Базовая фильтрация сообщений:

Исключение строк:

```
filebeat.inputs:
- type: docker
  ...
  exclude_lines: ['^DBG']
```

Включение строк:

```
filebeat.inputs:
- type: docker
  ...
  include_lines: ['^DBG']
```

Пример конфигурации filebeat

Вывод логов docker в elasticsearch:

```
output.elasticsearch:
  host: '${NODE_NAME}'
  hosts: 'elastic_server_ip_address:9200'
```

Ваши вопросы?

Маршрут вебинара

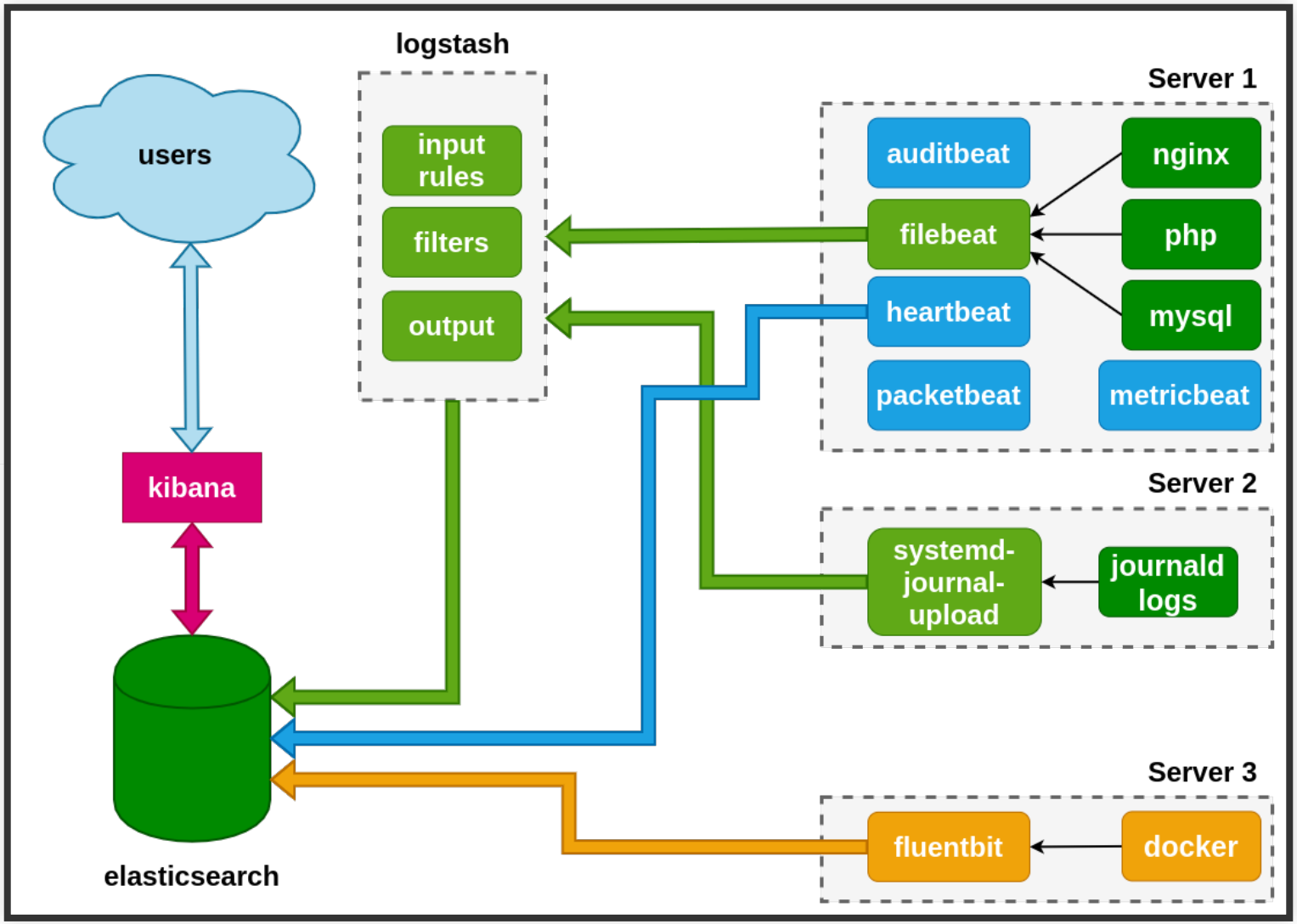
- Beats: Data shippers
- Heartbeat
- Auditbeat
- Metricbeat
- Filebeat
- Fluentbit

Fluentbit

Fluentbit - многоплатформенный opensource инструмент обработки логов, который призван стать "швейцарским ножом" для обработки и распространения журналов

https://docs.fluentbit.io

Fluentbit


logstash
input rules
filters
output
users
kibana
elasticsearch
Server 1
auditbeat
filebeat
heartbeat
packetbeat
nginx
php
mysql
metricbeat
Server 2
systemd-journal-upload
journald logs
Server 3
fluentbit
docker

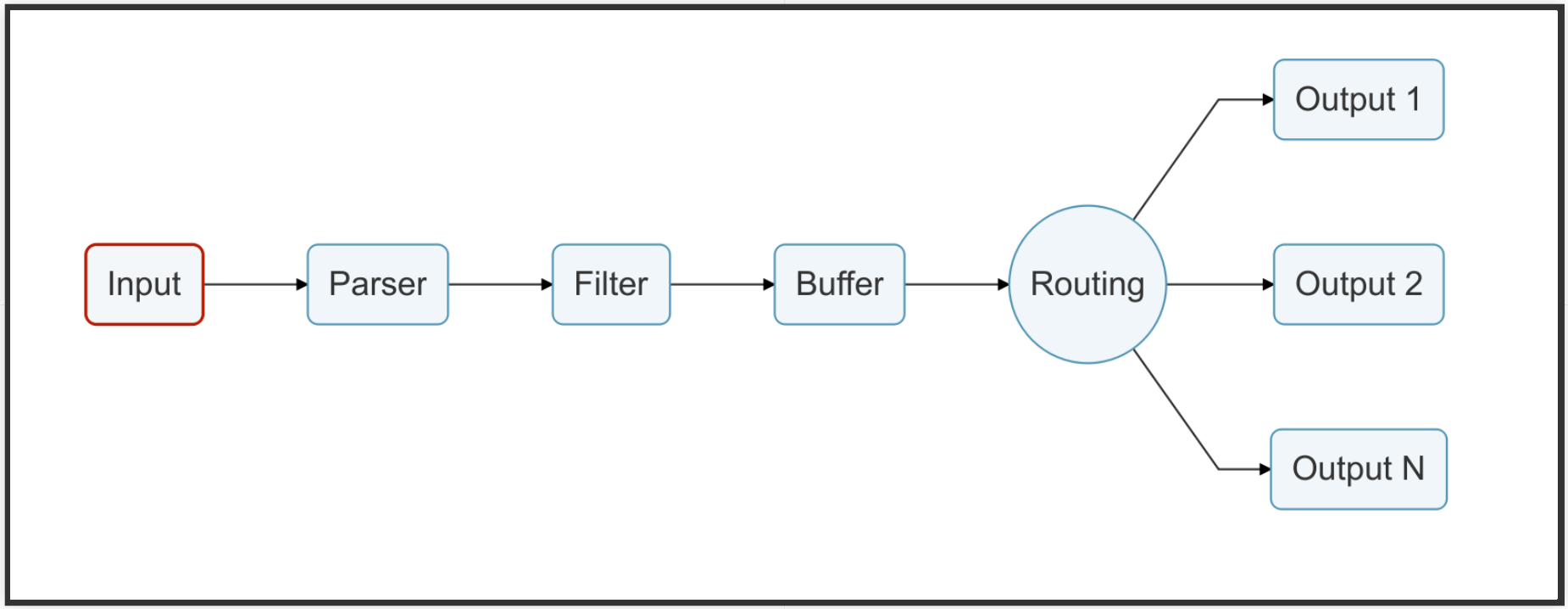
Fluentbit vs Fluentd

Основные отличия Fluentbit от Fluentd:

	Fluentd	Fluent Bit
Scope	Containers / Servers	Embedded Linux / Containers / Servers
Language	C & Ruby	C
Memory	~40MB	~650KB
Performance	High Performance	High Performance
Dependencies	Built as a Ruby Gem, it requires a certain number of gems.	Zero dependencies, unless some special plugin requires them.
Plugins	More than 1000 plugins available	Around 70 plugins available
License	Apache License v2.0	Apache License v2.0

Fluentbit

Конвеер данных fluentbit:



Fluentbit

Особенности:

- Высокая производительность работы
- Возможность структурировать сообщения с помощью JSON,Regex,LTSV and Logfmt
- Буферизация данных в процессе обработки
- Поддержка SSL/TLS
- Модульная архитектура с подключаемыми плагинами
- Можно писать свои фильтры на Lua или плагины выходных данных на Golang
- Адаптация под мониторинг с помощью Prometheus
- Балансировка выходных данных между несколькими upstream

Fluentbit

Варианты плагинов ввода данных

- docker events - события демона docker, получаемые из docker API
- exec - запуск сторонних сборщиков логов
- health - проверки внешних сервисов
- network i/o metrics - сбор статистики с сетевых интерфейсов системы
- syslog - сбор syslog сообщений через сетевые или unix сокеты

Fluentbit

Большой выбор плагинов ввода данных

- systemd - сбор сообщений от journald
- tail - мониторинг одного или нескольких файлов логов
- tcp - прием по протоколу TCP форматированных в JSON (или не форматированных вовсе) сообщений

Установка fluentbit

Установка репозитория:

```
vi /etc/repos.d/td-agent-bit.repo
[td-agent-bit]
name = TD Agent Bit
baseurl = https://packages.fluentbit.io/centos/7/$basearch/
gpgcheck=1
gpgkey=https://packages.fluentbit.io/fluentbit.key
enabled=1
```

Установка fluentbit:

```
yum install td-agent-bit
```

Конфигурация fluentbit

```
[SERVICE]
    flush        5
    daemon       Off
    log_level    info
    parsers_file parsers.conf
    plugins_file plugins.conf
    http_server  Off
    http_listen  0.0.0.0
    http_port    2020

[INPUT]
    Name   forward
    Listen 0.0.0.0
    Port   24224
```

Конфигурация fluentbit

```
[OUTPUT]
    Name  es
    Match *
    Host elk-lab-main
    Port 9200
    Index fluentbit
    Type  docker
```

Заполните, пожалуйста, опрос о занятии по ссылке в чате

Приходите на следующие вебинары

Спасибо за внимание!