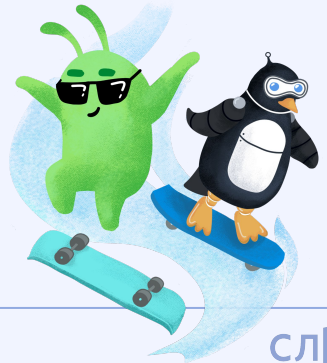
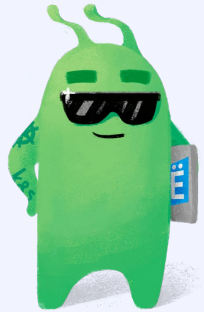
Мониторинг и логирование



Логирование

- Syslog
- Чтение файловых логов
- Ротация логов
- systemd-journald
- journalctl и работа с логами
- Централизованный сбор логов



Мониторинг

- atop
- Load Average
- Дисковая активность
- Сетевая активность
- Централизованный сбор показателей сервера

syslog

Стандарт отправки и регистрации сообщений

Определяет категории и приоритеты сообщений

Наиболее популярная реализация – rsyslog

rsyslog

Демон сбора и обработки логов

Названия логов между дистрибутивами часто отличаются

Конфигурация находится в /etc/rsyslog.conf

Конфигурация rsyslog

Правило обработки сообщения - **источник и приоритет**

Назначение - **куда** сообщение будет отправлено

Категории сообщений в syslog

- auth
- authpriv
- cron
- daemon
- kern
- lpr
- mail
- mark
- news
- security
- syslog
- user
- uucp
- local0..local7

Приоритеты сообщений syslog

- emerg
- alert
- crit
- err
- warning
- notice
- info
- debug

Как читать файловые логи

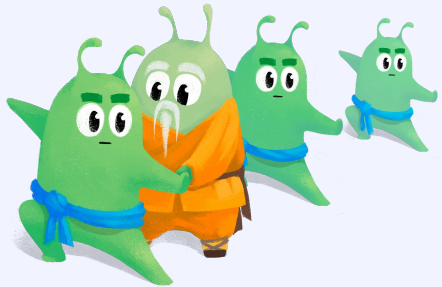
- **cat** – вывести содержимое файла
- **less** – постраничное чтение файла
- **tail** с ключом **-f** – вывод новых записей в консоль

Ротация логов

logrotate – утилита автоматической ротации логов

Конфиг – /etc/logrotate.conf

```
файл_лога {
        параметр1
        параметр2
        параметр3
}
```

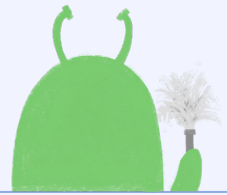


Параметры logrotate

- rotate
- create
- dateext
- compress
- delaycompress
- extension
- mail
- maxage
- missingok
- olddir
- postrotate/endscript
- start
- size

Интервалы ротации

- hourly
- daily
- weekly
- monthly
- yearly



systemd-journald

systemd-journald

Хранит логи в бинарном виде

Шифрует и архивирует журналы автоматически

Автоматически ротирует журналы

Все systemd-юниты по умолчанию пишут в journald

Конфигурация journald

Файл конфигурации – /etc/systemd/journald.conf

ForwardToSyslog – перенаправлять сообщения в syslog

Storage – место хранения журналов

Compress – переключатель архивирования журналов

Seal – переключатель шифрования файлов журналов

journalctl

Утилита для просмотра журналов
и управления journald

journalctl -b

Показать журналы с момента запуска

journalctl --list-boots

Выводит список журналов загрузок

Логирование на удаленный сервер

Удаленное логирование

- rsyslog
- journald
- fluent-bit / filebeat / logstash

Elasticsearch — система полнотекстового поиска и аналитики

Kibana — веб-интерфейс визуализации данных

EFbK / ELK

Набор приложений для организации логирования

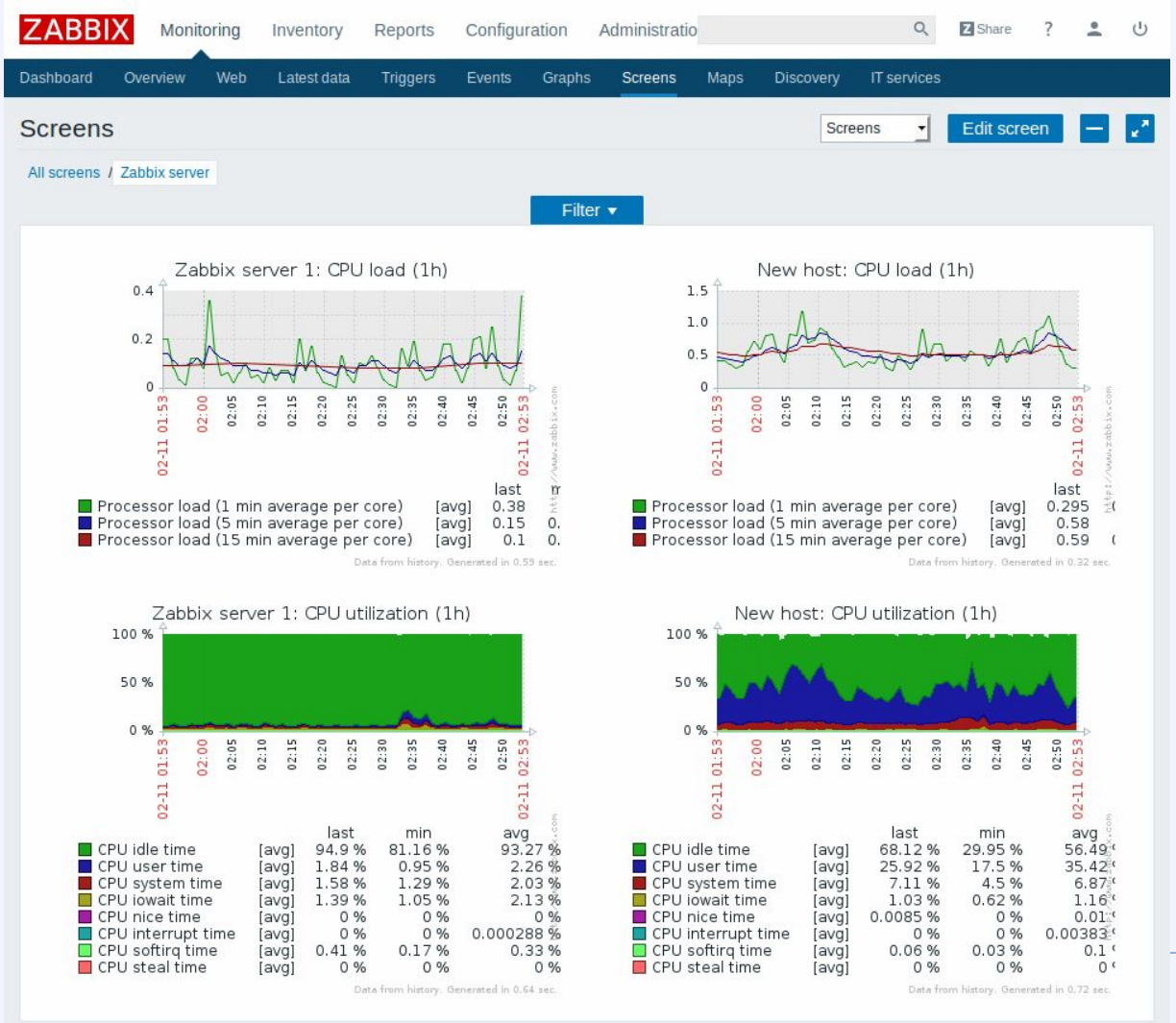
E — Elasticsearch

Fb — fluent-bit / filebeat

L — Logstash

K — Kibana

Мониторинг


ZABBIX
Monitoring
Inventory
Reports
Configuration
Administratio
Share
Dashboard
Overview
Web
Latest data
Triggers
Events
Graphs
Screens
Maps
Discovery
IT services
Screens
Screens
Edit screen
All screens / Zabbix server
Filter
Zabbix server 1: CPU load (1h)
Processor load (1 min average per core) [avg] 0.38
Processor load (5 min average per core) [avg] 0.15
Processor load (15 min average per core) [avg] 0.1
Data from history. Generated in 0.59 sec.
New host: CPU load (1h)
Processor load (1 min average per core) [avg] 0.295
Processor load (5 min average per core) [avg] 0.58
Processor load (15 min average per core) [avg] 0.59
Data from history. Generated in 0.32 sec.
Zabbix server 1: CPU utilization (1h)
last min avg
CPU idle time [avg] 94.9 % 81.16 % 93.27 %
CPU user time [avg] 1.84 % 0.95 % 2.26 %
CPU system time [avg] 1.58 % 1.29 % 2.03 %
CPU iowait time [avg] 1.39 % 1.05 % 2.13 %
CPU nice time [avg] 0 % 0 % 0 %
CPU interrupt time [avg] 0 % 0 % 0.000288 %
CPU softirq time [avg] 0.41 % 0.17 % 0.33 %
CPU steal time [avg] 0 % 0 % 0 %
Data from history. Generated in 0.64 sec.
New host: CPU utilization (1h)
last min avg
CPU idle time [avg] 68.12 % 29.95 % 56.49
CPU user time [avg] 25.92 % 17.5 % 35.42
CPU system time [avg] 7.11 % 4.5 % 6.87
CPU iowait time [avg] 1.03 % 0.62 % 1.16
CPU nice time [avg] 0.0085 % 0 % 0.01
CPU interrupt time [avg] 0 % 0 % 0.00383
CPU softirq time [avg] 0.06 % 0.03 % 0.1
CPU steal time [avg] 0 % 0 % 0
Data from history. Generated in 0.72 sec.


fren
Last 5 minutes
5s
datasource
Prometheus
Job
node
Host:
fragile.local
Port
9100
Health
CPU Load
60%
CPU Temperature
42 °C
RAM Used
26%
Drive health
OK
Network Utilization (Hourly)
Last 24 hours
4.7 GiB
3.7 GiB
2.8 GiB
1.9 GiB
954 MiB
0 B
14:00
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00
08:00
10:00
12:00
received
sent
Drive temperatures
/dev/sda
35 °C
/dev/sdb
35 °C
/dev/sdc
37 °C
Free storage
11.72 TB
Per Container CPU Usage
100%
80%
60%
40%
20%
0%
13:18:00
13:18:30
13:19:00
13:19:30
13:20:00
13:20:30
13:21:00
13:21:30
13:22:00
13:22:30
max
avg
Jellyfin 0% 0%
Deluge 40% 20%
Grafana 5% 0%
InfluxDB 7% 0%
Radarr 0% 0%
Sonarr 0% 0%
Uptime
1.2 hours
Download
64 Mbps
Upload
9.1 Mbps
Ping
79 ms
Fan speed
CPU fan
1000
Case fan
939

В следующей серии

Безопасность в Linux