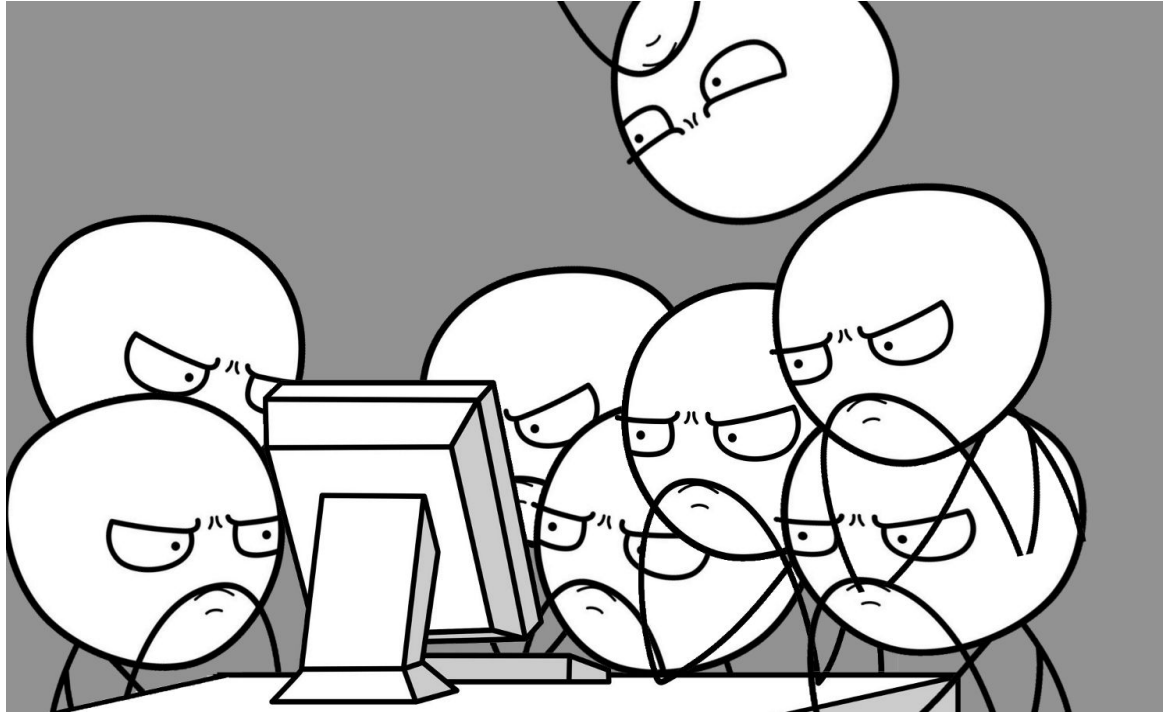


Мониторинг системы мониторинга



Кто мы и о чём расскажем в докладе

Часть 1. Мир Splunk

Рассказывает: Михаил Ефремов, системный администратор/devops

Часть 2. Make business monitoring great again

Рассказывает: Анна Манакова, системный администратор/devops

Часть 3. Данные о данных: Yet Another CMDB

Рассказывает: Михаил Ефремов

Часть 1. Мир Splunk

О чём расскажем в этой части:

- Мотивация доклада (чем хотим поделиться)
- «Категории» мониторинга
- Splunk как экосистема (в которой уживаются данные и код)
- Splunk как аппаратно-программный комплекс

Мотивация доклада (чем хотим поделиться)



Мотивация доклада (чем хотим поделиться)



Мотивация доклада (чем хотим поделиться)

Ощущение удовлетворения :)

Категории мониторинга

- Инфраструктурный мониторинг
- Бизнес-мониторинг

Экосистема Splunk

Splunk это

- Хранилище данных
- Средство разработки

Экосистема Splunk

Splunk как хранилище данных

- Логоподобные данные
- Справочники (lookups)
 - Файлы
 - Коллекции в MongoDB

Экосистема Splunk

Splunk как средство разработки

- Приложения, работающие в контексте самого Splunk
- REST API для интеграции с другими системами

Экосистема Splunk

Что ещё

- SPL (Search Processing Language)
 - Вычисляемые налету поля
 - Conditions
 - Regex
 - Статистические функции
 - Relational operators
 - Transactions processing
 - Predictions
 - и др.

Экосистема Splunk

Что ещё

- UI
 - Алерты
 - Отчёты
 - Реалтайм дашборы

Экосистема Splunk

Что хочет бизнес?

- Изощрённейшая аналитика с красивыми картинками
- Алерты по всему!
- Прямо сейчас!!

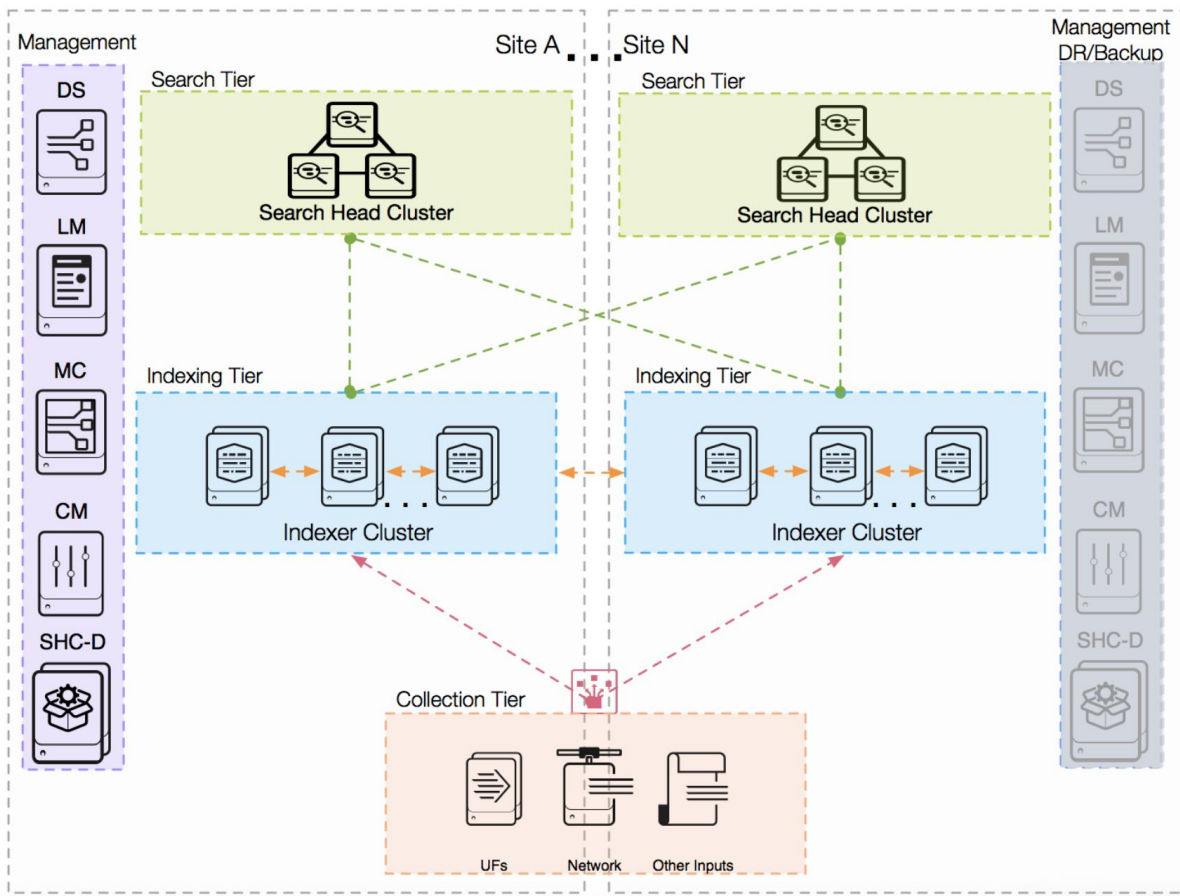
Прямо сейчас!!1



Splunk как аппаратно-программный комплекс

- Кластеры indexer-ов
- Кластеры search head-ов
- Служебные машины
- Источники данных

Splunk как аппаратно-программный комплекс



Splunk как аппаратно-программный комплекс

Индексеры

- Полтора десятка железных серверов
- Сотни гиг RAM на каждом
- Десятки ядер (Xeon) на каждом
- NVME/SSD для горячих и тёплых данных
- 10+ терабайтные локальные RAID
- Резервирование: податацентровое + реплики внутри ДЦ

Splunk как аппаратно-программный комплекс

Search head-ы

- Примерно то же самое, но без забористых хранилок

Splunk как аппаратно-программный комплекс

Источники

- DBconnect
-
-
-
-

Splunk как аппаратно-программный комплекс

Источники

- DBconnect
- Syslog
-
-
-

Splunk как аппаратно-программный комплекс

Источники

- DBconnect
- Syslog
- HTTP Event Collector
-
-

Splunk как аппаратно-программный комплекс

Источники

- DBconnect
- Syslog
- HTTP Event Collector
- Universal Forwarders
-

Splunk как аппаратно-программный комплекс

Источники

- DBconnect
- Syslog
- HTTP Event Collector
- Universal Forwarders
- Кое-что ещё...

Splunk как аппаратно-программный комплекс

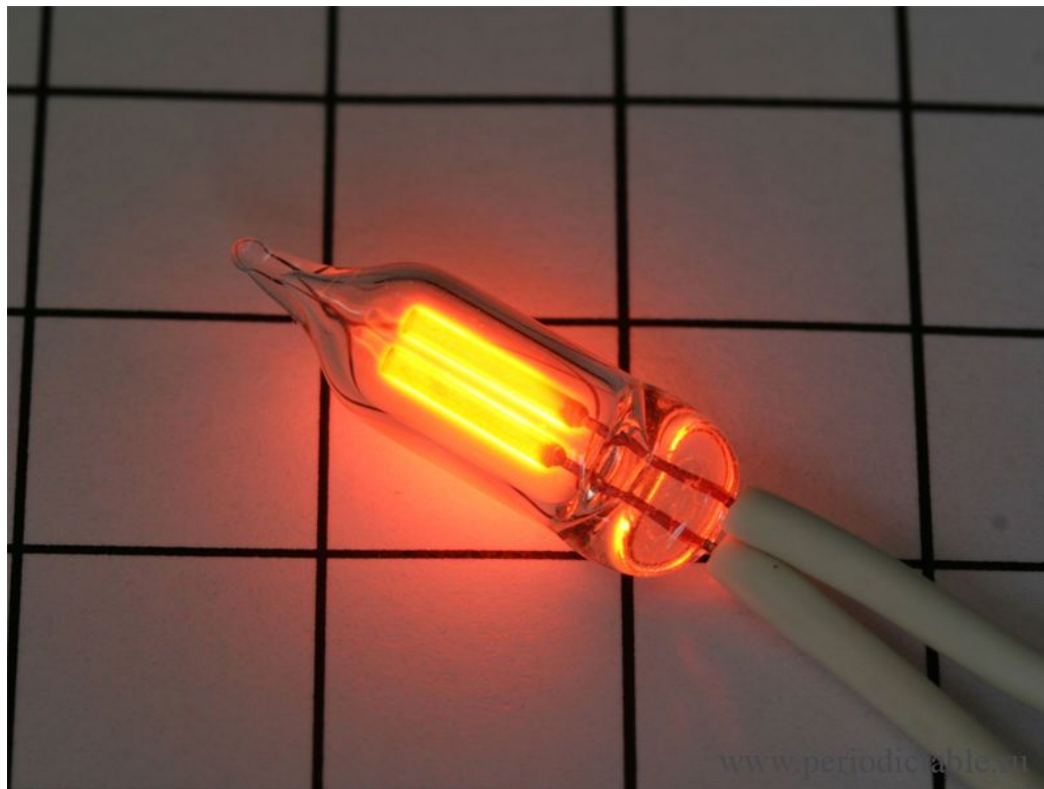
Ещё немного цифр

- Терабайты данных суммарно в сутки
- Несколько тысяч источников
- Сотни активных пользователей
- Сотни RPS, десятки SPS
- Хранение в среднем пару недель

Splunk как аппаратно-программный комплекс

А что же внутри?

Splunk как аппаратно-программный комплекс



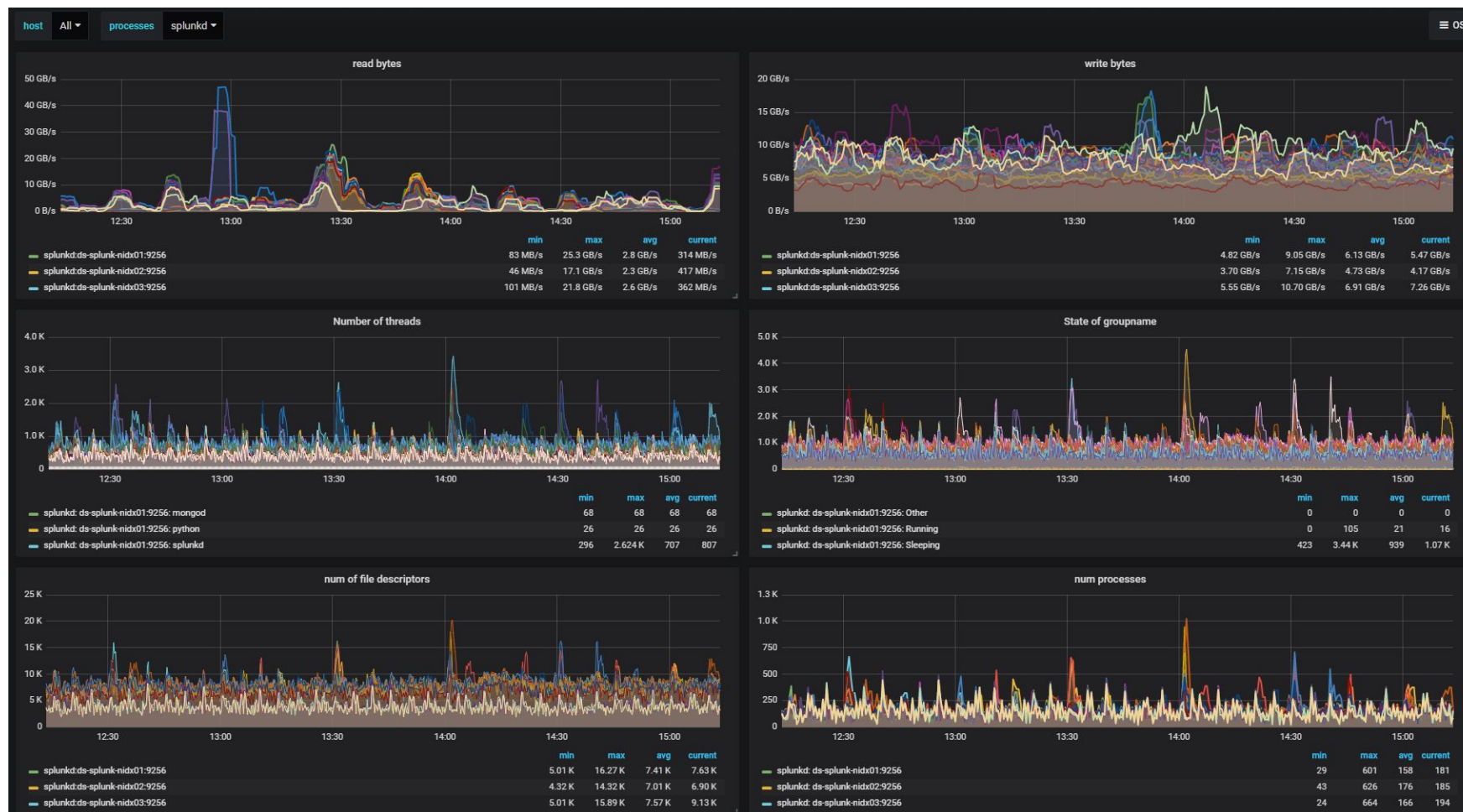
И в какой-то момент что-то пошло не так...

Часть 2. Make Business Monitoring Great Again

О чём расскажем в этой части:

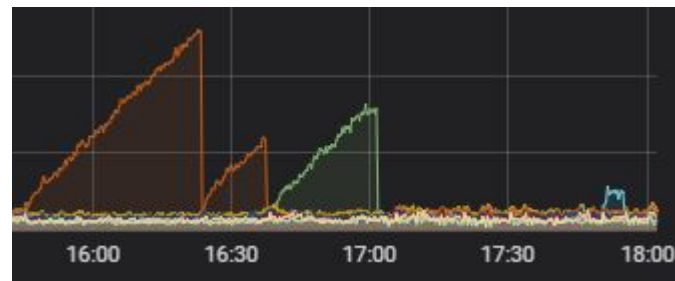
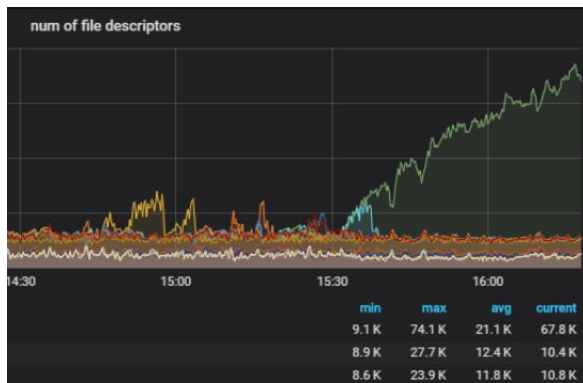
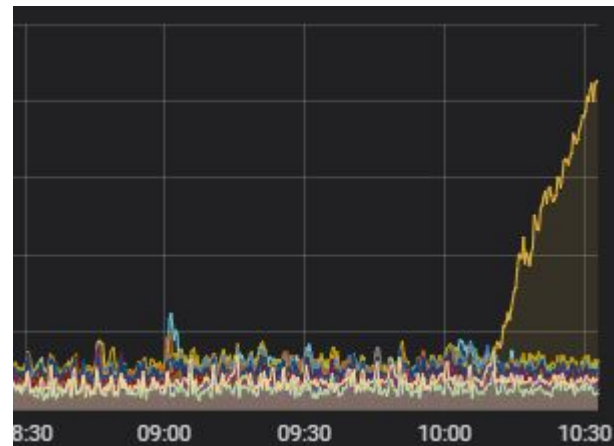
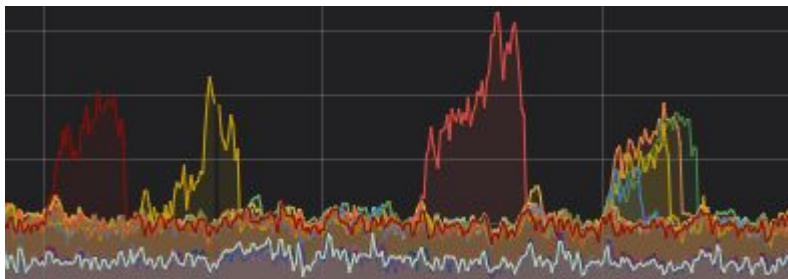
- Формулировка проблемы
- Мониторинг процессов, что нас удивило и где нашли зацепку
- Жизнь внутри индекса и как за этим можно смотреть

Мониторинг процессов



<https://github.com/ncabatoff/process-exporter>

В начале было...



Помоги себе сам

Monitoring User

Health Status of Splunkd

splunkd

File Monitor Input

- BatchReader-0
- BatchReader-1
- BatchReader-2
- BatchReader-3
- TailReader-0
- TailReader-1
- TailReader-2
- TailReader-3

Index Processor

- Buckets**
- Disk Space
- Index Optimization

Indexer Clustering

- Master Connectivity
- Replication Failures
- Slave State
- Slave Version

Buckets

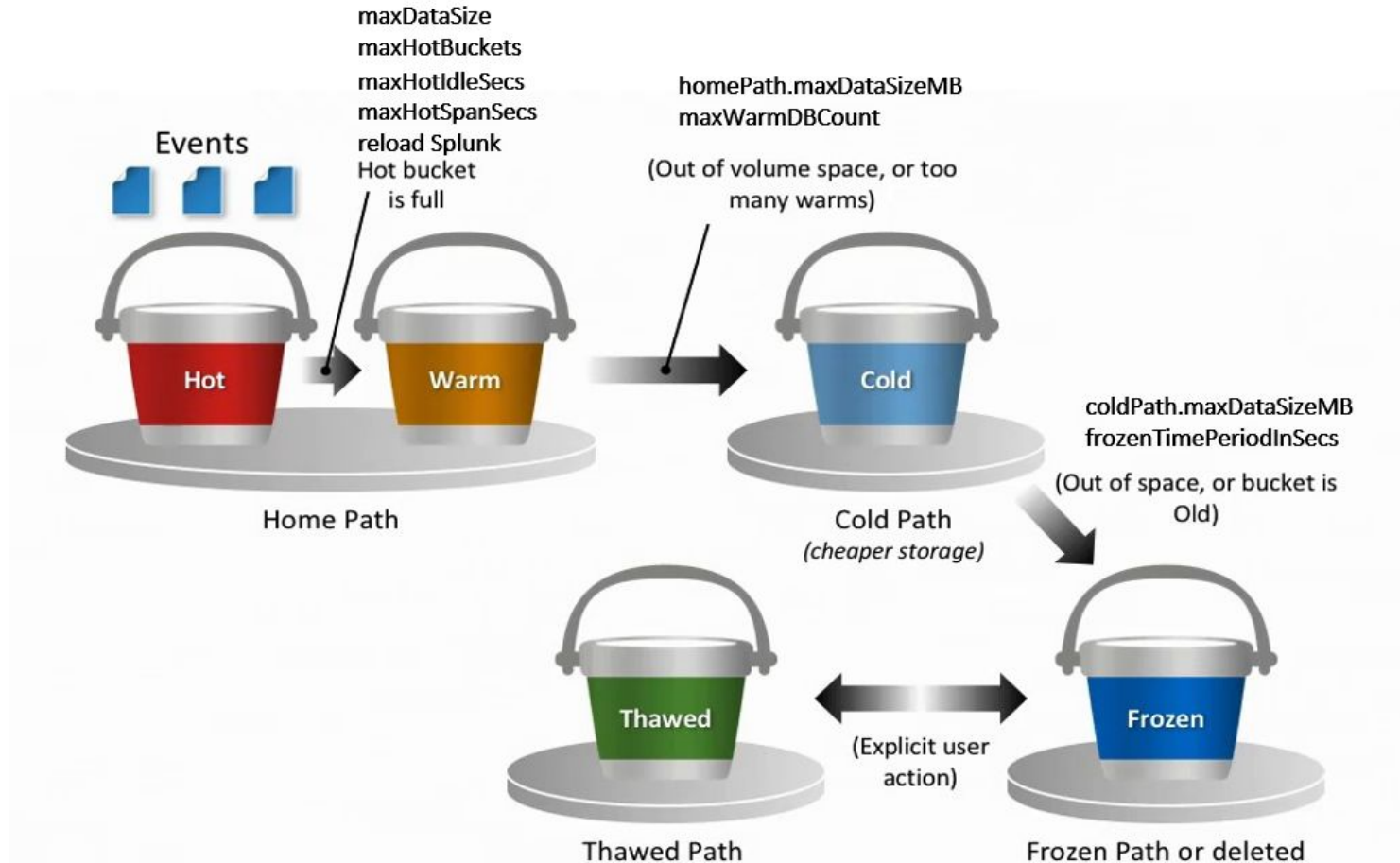
Root Cause(s):

- The percentage of small of buckets created (100) over the last hour is very high and exceeded the red thresholds (50) for index=jasper, and possibly more indexes, on this indexer

Last 50 related messages:

- 07-30-2019 13:23:13.341 +0300 INFO HotBucketRoller - finished moving hot to warm bid=ibul~13285~F79A06D1-E3FA-4855-AD58-9A3F5676F1FC idx=ibul from=hot_v1_13285 to=db_1563807605_1563807605_13285_F79A06D1-E3FA-4855-AD58-9A3F5676F1FC size=49152 caller=trimDb:chillWarm_rollHot isinit=false selective=false
- 07-30-2019 13:10:19.936 +0300 INFO HotBucketRoller - finished moving hot to warm bid=integration~6952~F79A06D1-E3FA-4855-AD58-9A3F5676F1FC idx=integration from=hot_v1_6952 to=db_1564467386_1564409286_6952_F79A06D1-E3FA-4855-AD58-9A3F5676F1FC size=1089003520 caller=trimDb:chillWarm_rollHot isinit=false selective=false
- 07-30-2019 13:09:08.070 +0300 INFO HotBucketRoller - finished moving hot to warm bid=integration~6953~F79A06D1-E3FA-4855-AD58-9A3F5676F1FC idx=integration from=hot_v1_6953 to=db_1564466075_1564413881_6953_F79A06D1-E3FA-4855-AD58-9A3F5676F1FC size=751292416 caller=trimDb:chillWarm_rollHot isinit=false selective=false
- 07-30-2019 13:08:03.625 +0300 INFO HotBucketRoller - finished moving hot to

Жизненный цикл данных в индексе



Откуда горки растут

[filenet]

```
homePath = $SPLUNK_DB/cl_filenet/db
coldPath = $SPLUNK_DB/cl_filenet/coldddb
thawedPath = $SPLUNK_DB/cl_filenet/thaweddb
maxHotBuckets = 10
maxHotIdleSecs = 86400
repFactor = auto
maxDataSize = auto_high_volume
maxTotalDataSizeMB = 500
```

$\text{homePath.maxDataSizeMB} = (\text{maxWarmDBCount} + \text{maxHotBuckets}) * \text{maxDataSize}$

$\text{coldPath.maxDataSizeMB} = \text{maxTotalDataSizeMB} - \text{homePath}$

Status

Data Age vs Frozen Age (days) ▾

348 / 2184

Index Usage (GB) ▾

7.06 / 0.49

Home Path Usage (GB) ▾

0 / unlimited

Cold Path Usage (GB) ▾

0 / unlimited

The columns use attributes specified in [indexes.conf](#).

- **Data Age vs Frozen Age:** The first value is based on the age of the oldest event in the index. The second value is derived from the attribute frozenTimePeriodInSecs.
- **Index Usage:** The first value is the current size of the index. The second value is the index capacity, as specified in maxTotalDataSizeMB.
- **Home Path Usage:** The first value is the current size of the home path portion of the index. The second value is the home path capacity, as specified in homePath.maxDataSizeMB.
- **Cold Path Usage:** The first value is the current size of the cold path portion of the index. The second value is the cold path capacity, as specified in coldPath.maxDataSizeMB.

«Что делать?»

1. Для горячих бакетов ключевой параметр - *maxDataSize*:

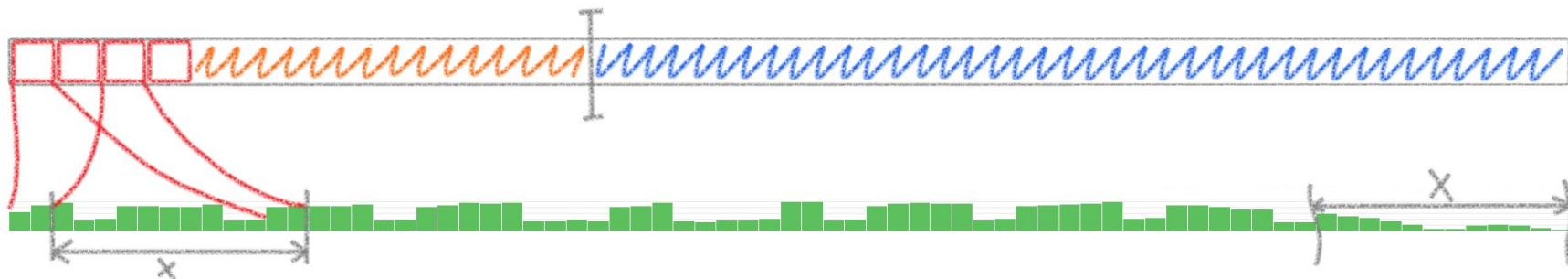
$$\limsup_{maxDataSize \rightarrow \infty} maxHotBuckets$$

2. Для теплых бакетов ключевой параметр - *homePath*:

$$\limsup_{maxDataSize \rightarrow 0} maxWarmDBCount$$

3. Исключается *maxHotIdleSecs* = 0:

$$\limsup_{maxHotSpanSecs \rightarrow x} maxDataSize$$



Результат внутреннего мониторинга сейчас

The screenshot displays the 'Health Status of Splunkd' window. At the top right, it shows 'Monitoring User' with a dropdown arrow. The window is divided into two main sections. The left section, titled 'splunkd', lists several components under different categories: 'File Monitor Input' (BatchReader-0 to -3, TailReader-0 to -3), 'Index Processor' (Buckets, Disk Space, Index Optimization), and 'Indexer Clustering' (Master Connectivity, Replication Failures, Slave State, Slave Version). Each component has a green information icon. The right section, titled 'Buckets', contains the text 'This feature is functioning correctly.' with a green information icon. A close button (X) is located in the top right corner of the window.

Monitoring User

Health Status of Splunkd

splunkd

File Monitor Input

- BatchReader-0
- BatchReader-1
- BatchReader-2
- BatchReader-3
- TailReader-0
- TailReader-1
- TailReader-2
- TailReader-3

Index Processor

- Buckets**
- Disk Space
- Index Optimization

Indexer Clustering

- Master Connectivity
- Replication Failures
- Slave State
- Slave Version

Buckets

This feature is functioning correctly.

Часть 3. Данные о данных: Yet Another CMDb

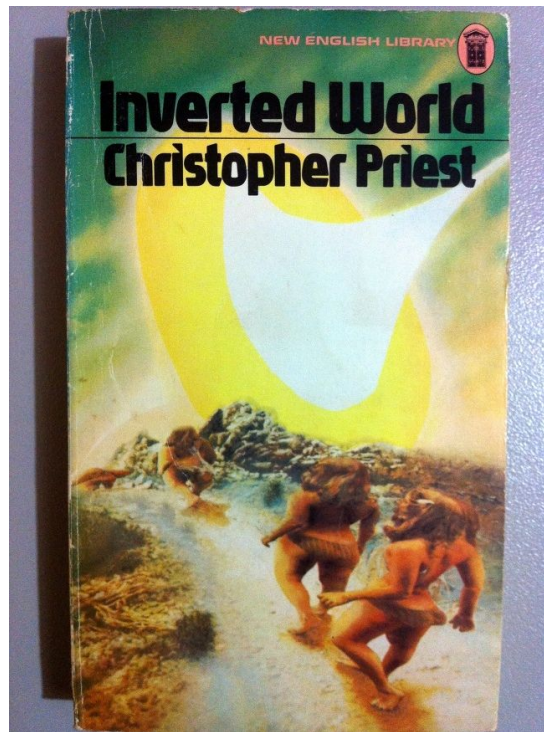


Часть 3. Данные о данных: Yet Another CMDB

О чём (не)расскажем в этой части:

- Summary по предыдущей части
- Затупившаяся бритва Оккама как мотивация создания Splunk CMDB
- Splunk REST API → Django-based CMDB
- CMDB → Splunk и связанная с этим «девопсня»

Ответ на загадку



Спасибо за внимание!

Докладывали обстановку

- Ефремов Михаил - e-mail: meechanic@gmail.com, telegram: @mike_meechanic
- Манакова Анна - e-mail: manakova.anna@gmail.com, telegram: @mannabanana

