

Splunk 7.0 新特性介绍

宋菲娅

3/30/2018



目录

1. 指标存储

2. 事件注释

3. 性能改进



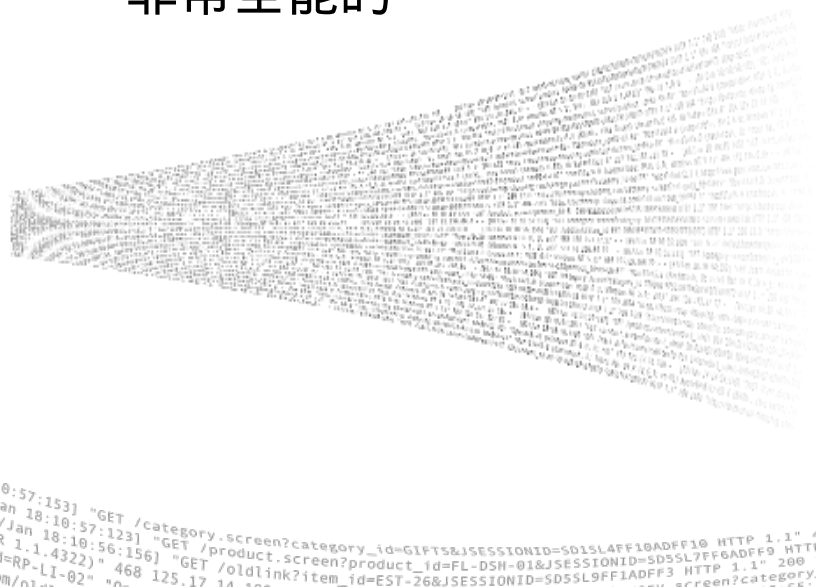
指标存储

Splunk 7.0 新特性

事件 vs 指标

事件

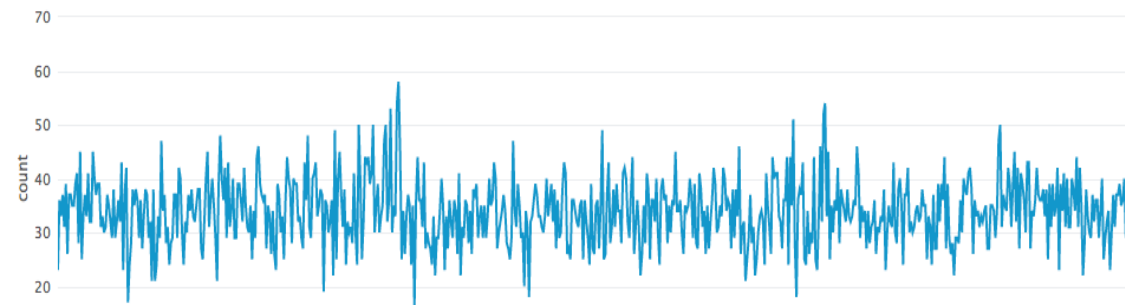
- 非结构化数据
- 大海捞针
- 能解释“为什么”
- 回答可能还没有发生的问题
- 非常全能的



```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFT&SESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Mozilla/5.0" "Opera/9.20 (Win  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FFADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=SD18SL8FFADFF9 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-6&product_id=FI-SW-03" "Opera/9.20 (Win  
ows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=RP-LI-02" "Mozilla/5.0" "Opera/9.20 (Win  
buttercup-shopping.com/cart.do?action=purchase&itemId=RP-LI-02" "Mozilla/5.0" "Opera/9.20 (Win
```

指标

- 结构化数据
- 观察过程或设备的最佳方法
- 做监测的可靠的方法
- 知道想要测量什么
- 特定场景，例如 CPU 使用率、网络延迟、用户数量等



指标组成元素



时间



指标名称

system.cpu.idle



测量

数字类型数据



维度

host=www.h1.com

region=us-east-1

instancetype=d2.8xl

Splunk 提供一个统一平台 分析事件及指标

指标存储

- ▶ **Splunk 内置**
- ▶ **新建索引时设置**
- ▶ **透明的平台支持**
 - RBAC
 - 集群
 - 索引管理
- ▶ **高度优化**
 - 查询速度
 - 摄取速度

新索引

常规设置

索引名称

设置索引名称 (例如, INDEX_NAME)。使用 index=INDEX_NAME 搜索。

索引数据类型

事件

指标

要存储的数据类型 (基于事件或指标)。

起始路径

热/温数据库路径。保留空白将使用默认设置 (\$SPLUNK_DB/INDEX_NAME/db)。

冷路径

冷数据库路径。保留空白将使用默认设置 (\$SPLUNK_DB/INDEX_NAME/colddb)。

解冻的路径

解冻/恢复数据库路径。保留空白将使用默认设置 (\$SPLUNK_DB/INDEX_NAME/thaweddb)。

整个索引的最大大小

500

GB

▼

整个索引的最大目标大小。

热/温/冷数据桶的最大大小

auto

GB

▼

数据桶的最大目标大小。输入 'auto_high_volume' 表示大容量索引。

冻结的路径

冻结的数据桶存档路径。如果您需要 Splunk 自动存档冻结的数据桶, 请设置此项。

应用

Search & Reporting

▼

取消

保存

指标索引

| 域 (Field) | 是否必须 | 描述 | 举例 |
|-----------------------|------|-----------------------|---|
| metric_name | 是 | 指标名称 | os.cpu.idle |
| _time | 是 | 指标测量的时间 (UNIX 时间戳) | 1505322000 |
| _value | 是 | 指标测量的结果 (浮点数) | 41.1234 |
| < 维度 A>... < 维度 Z> | 不是 | 任意数目的维度描述 | Field: ip; Value: 10.2.1.166 |

指标搜索命令 - mstats

- ▶ 语法

| **mstats** <stats-function> ...

WHERE index=<metric_index> **AND** metric_name=<metricname> ...

[span=<timespan>] [**BY|GROUPBY** <metricname|dimension>]

- ▶ 分析指标数据函数 <stats-function> ，作用在 `_value` 字段上

avg(), count(), max(), median(), min(), sum()...

- ▶ 支持历史搜索（磁盘数据）和实时搜索（内存数据）

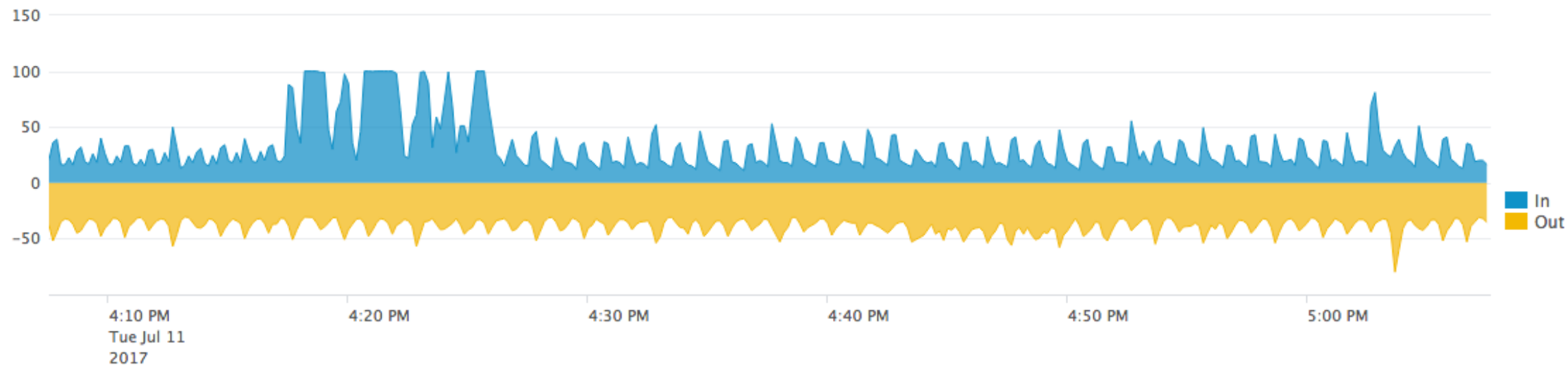
指标搜索命令 - mstats

| **mstats** avg(_value) **WHERE** metric_name="network.*" **span**=10s **BY** metric_name

| **timechart** avg(_value) **span**=10s **BY** metric_name

| **rename** network.rx **AS** In, network.tx **AS** Out

| **eval** Out = -Out



度量目录

- ▶ SPL – mcatalog
- ▶ 作用在 metric_name 和 dimension 域
- ▶ 列出目录信息
(e.g. 指标名称, 维度信息)
- ▶ 语法

| **mcatalog** values(<field>) ...

[**WHERE** index=<metric_index>

AND metric_name=<metricname> ...]

[**BY** <metricname|dimension>]

- ▶ REST endpoint

- 列出指标名称

/services/catalog/metricstore/metrics

- 列出维度名称 :

/services/catalog/metricstore/dimensions

- 列出维度上的值 :

/services/catalog/metricstore/dimensions
/{name}/values

导入指标数据的方法

► StatsD

- 通过 TCP/UDP 传输

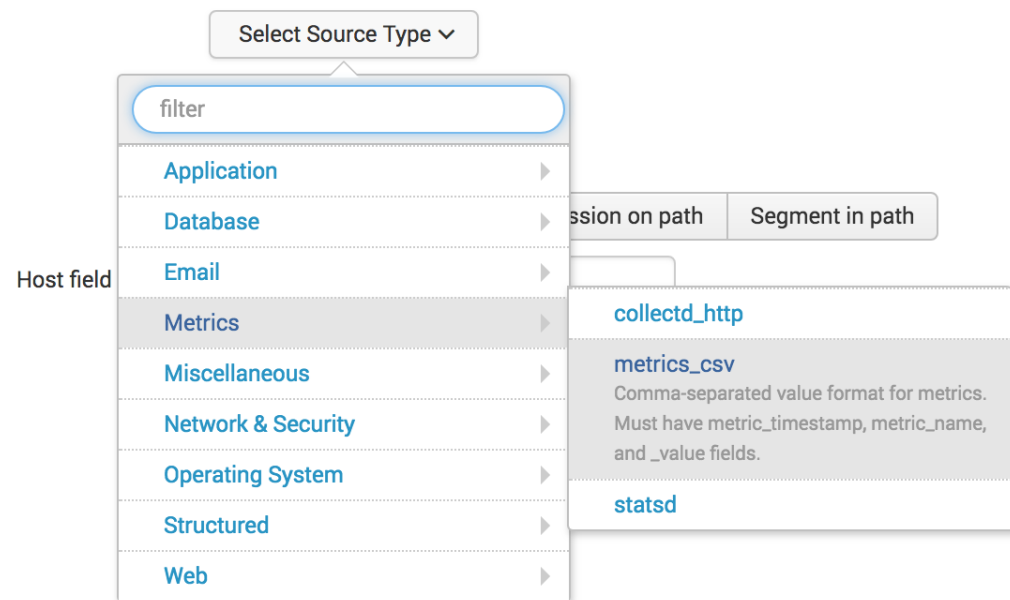
- StatsD line metric protocol

<metric_name>:<_value>|<metric_type>|
#dim1:valueX,dim2:valueY

► CollectD

- 结合 write_http 插件使用
- 通过 HTTP Event Collector 传输

► csv 文件导入



► 定制 source type

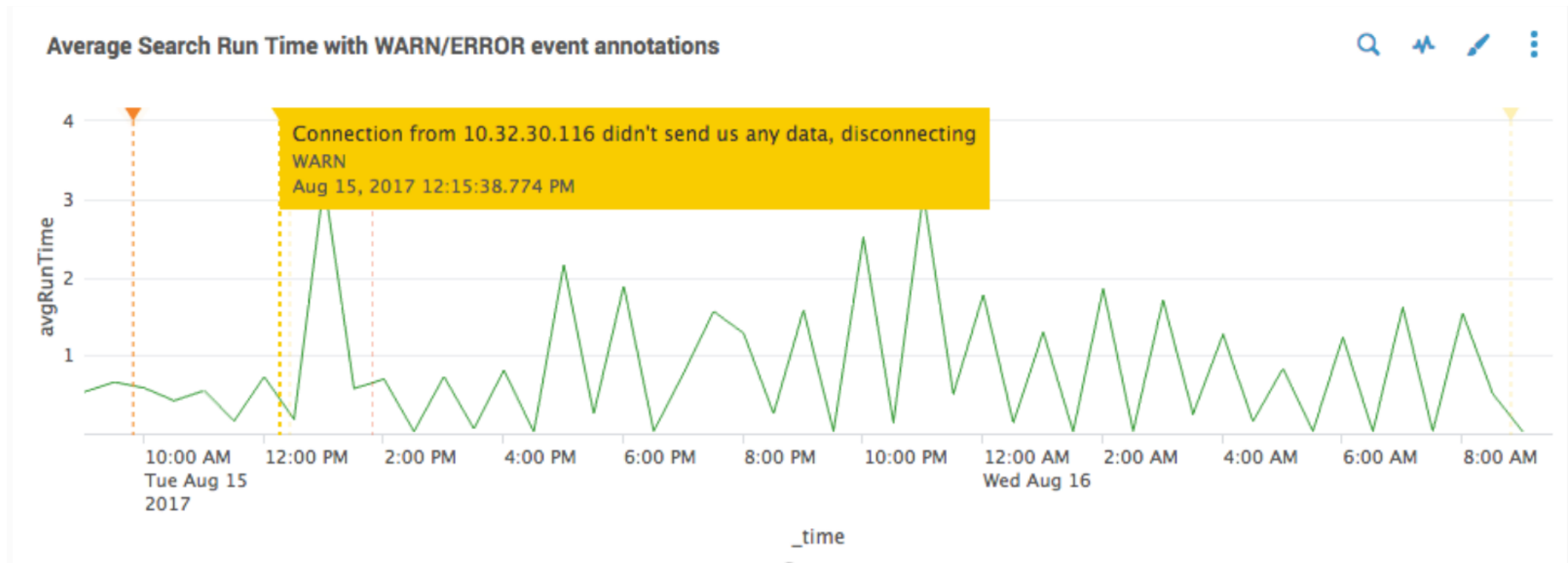
- props.conf
- transforms.conf

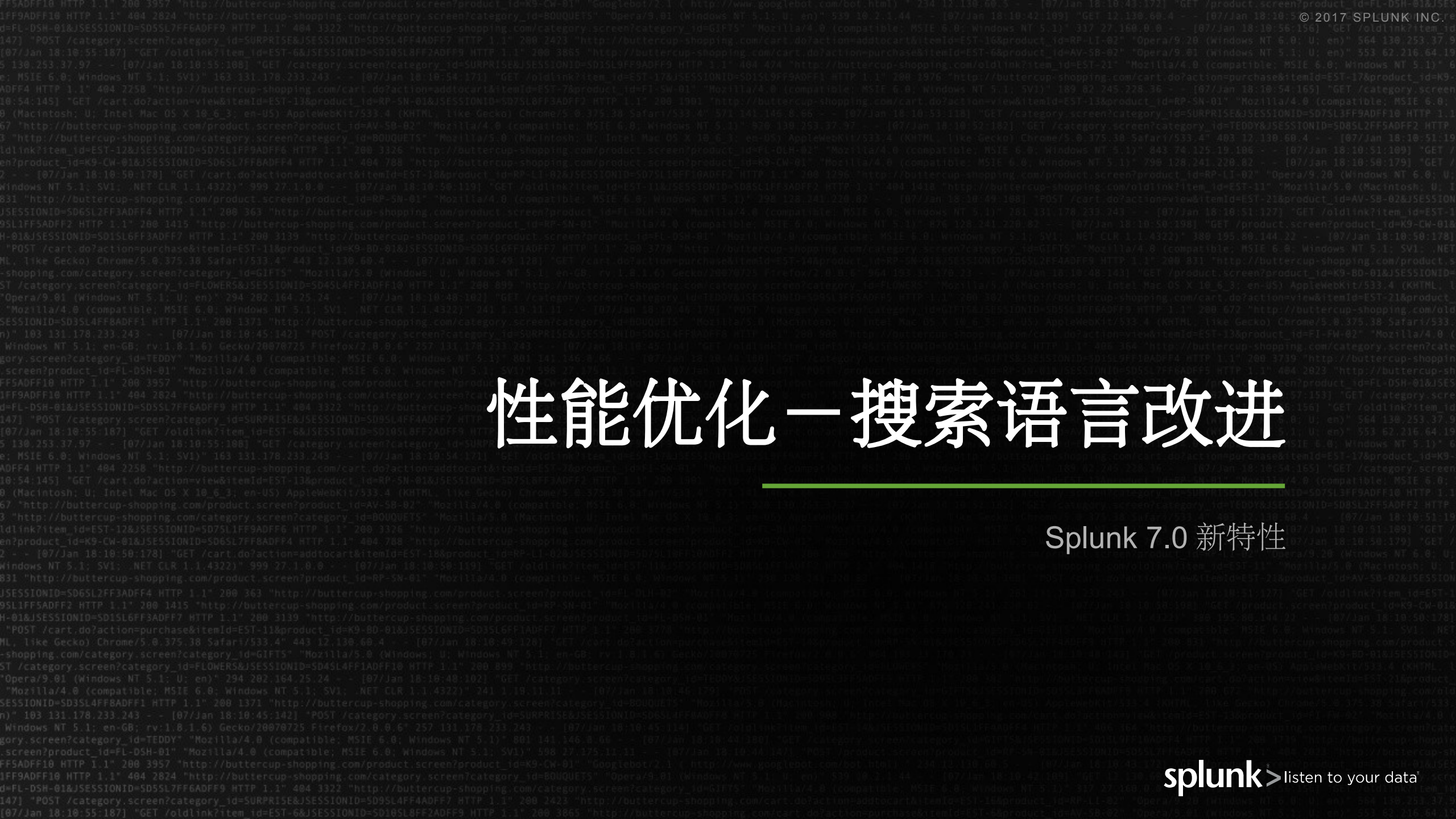
性能对比

- ▶ 指标索引比事件索引减少 **50%** 磁盘空间使用量
- ▶ 搜索速度比加速后的日志数据提升 **20** 倍
- ▶ 搜索速度比未加速的日志数据提升 **100** 倍

事件注释

- ▶ 一个图表中结合两种搜索结果
- ▶ 为变化趋势提供上下文解释
- ▶ 更加深入地洞察数据





性能优化—搜索语言改进

Splunk 7.0 新特性

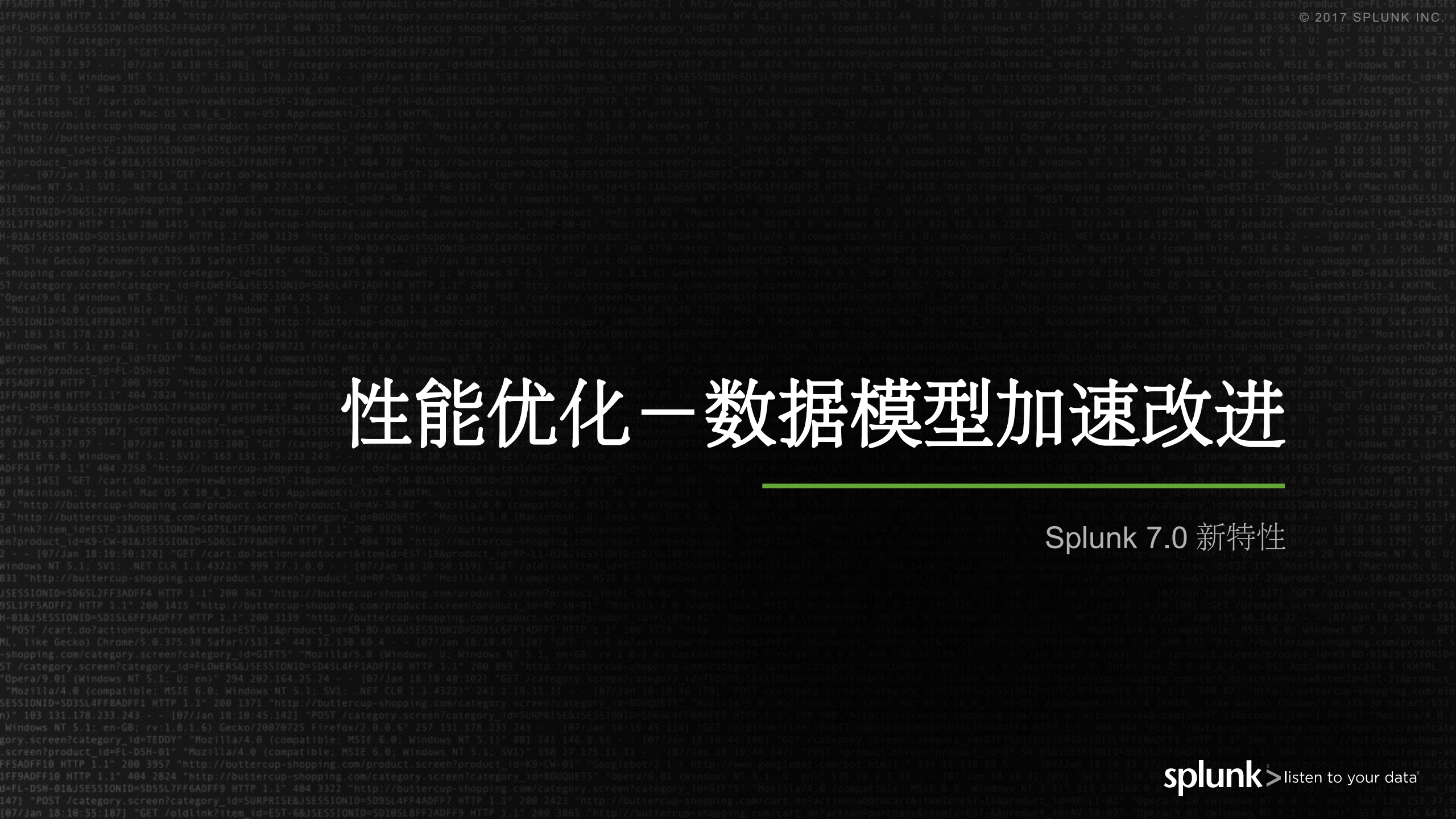
搜索执行时间分析

一个典型的安装了多个 TA 的 Splunk 环境



搜索指令 - DIRECTIVES

- ▶ 产生 Tags 和 Eventtypes 很费时
 - 搜索返回的每一个结果都会在所有 Tags 和 Eventtypes 上做过滤
 - 当一个 Splunk 的环境里安装了多个 TA，它可以占据超过 50% 的执行时间
- ▶ Splunk7.0 提供一种新的方法来限定 Tags/Eventtypes
 - search 500 DIRECTIVES(REQUIRED_TAGS(tags="foo, bar"))
 - search 500 DIRECTIVES(REQUIRED_EVENTTYPES(eventtypes="alpha,omega"))
- ▶ 合并指令
 - search 500 DIRECTIVES(REQUIRED_EVENTTYPES(eventtypes="alpha,omega"),REQUIRED_TAGS(tags="foo,bar"))
- ▶ 影响
 - 对搜索结果集较小的搜索影响不大
 - 对搜索结果集较大的搜索影响很大



性能优化—数据模型加速改进

Splunk 7.0 新特性

数据模型应用场景

- 数据集与语义知识的结构化映射
- 构建者 — 了解数据结构和 **SPL** 语言
- 使用者 — 数据透析表

CONSTRAINTS

```
index=_internal source=*scheduler.log* OR source=*metrics.log* OR
source=*splunkd.log* OR source=*license_usage.log* OR
source=*splunkd_access.log*
```

Constraint

CONSTRAINTS

```
index=_internal source=*scheduler.log* OR source=*metrics.log* OR
source=*splunkd.log* OR source=*license_usage.log* OR
source=*splunkd_access.log*
source=*scheduler.log*
```

Inherited

Constraint

EVENTS

Splunk Server

Scheduler

Alerts

Scheduled Reports

Summary Indexing Searches

Acceleration

Data Model Acceleration

Report Acceleration

Licenser

Daily Usage Summary

Daily Slave Warning Summary

Quota Usage

Pool Warnings

data*

数据模型加速

- ▶ 加速范围（以当前时间为参考）
- ▶ 每隔一定时间，更新加速文件
- ▶ 生成时间序列索引文件 (.tsidx)
- ▶ 占用额外的磁盘空间

Edit Acceleration

Data Model Alerts

Accelerate ☒

Acceleration may increase storage and processing costs.

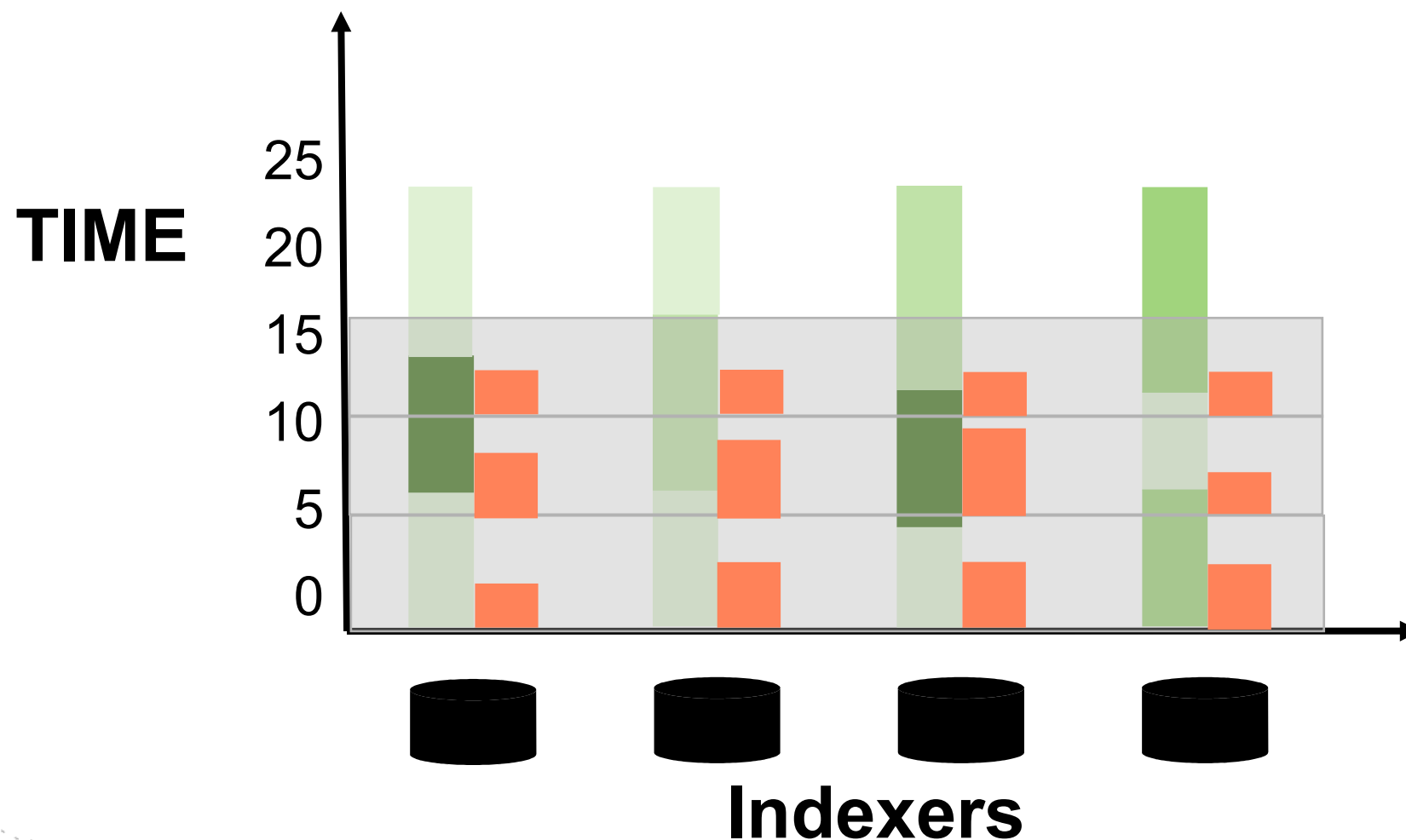
Summary Range? 1 Day ▼

- ✓ 1 Day
- 7 Days
- 1 Month
- 3 Months
- 1 Year
- All Time
- Custom

Cancel Save

data model Edit Pivot

数据模型加速工作原理



TIME



Indexers

数据模型加速 (Data Model Acceleration)

问题和解决方法

► Splunk 7.0 之前

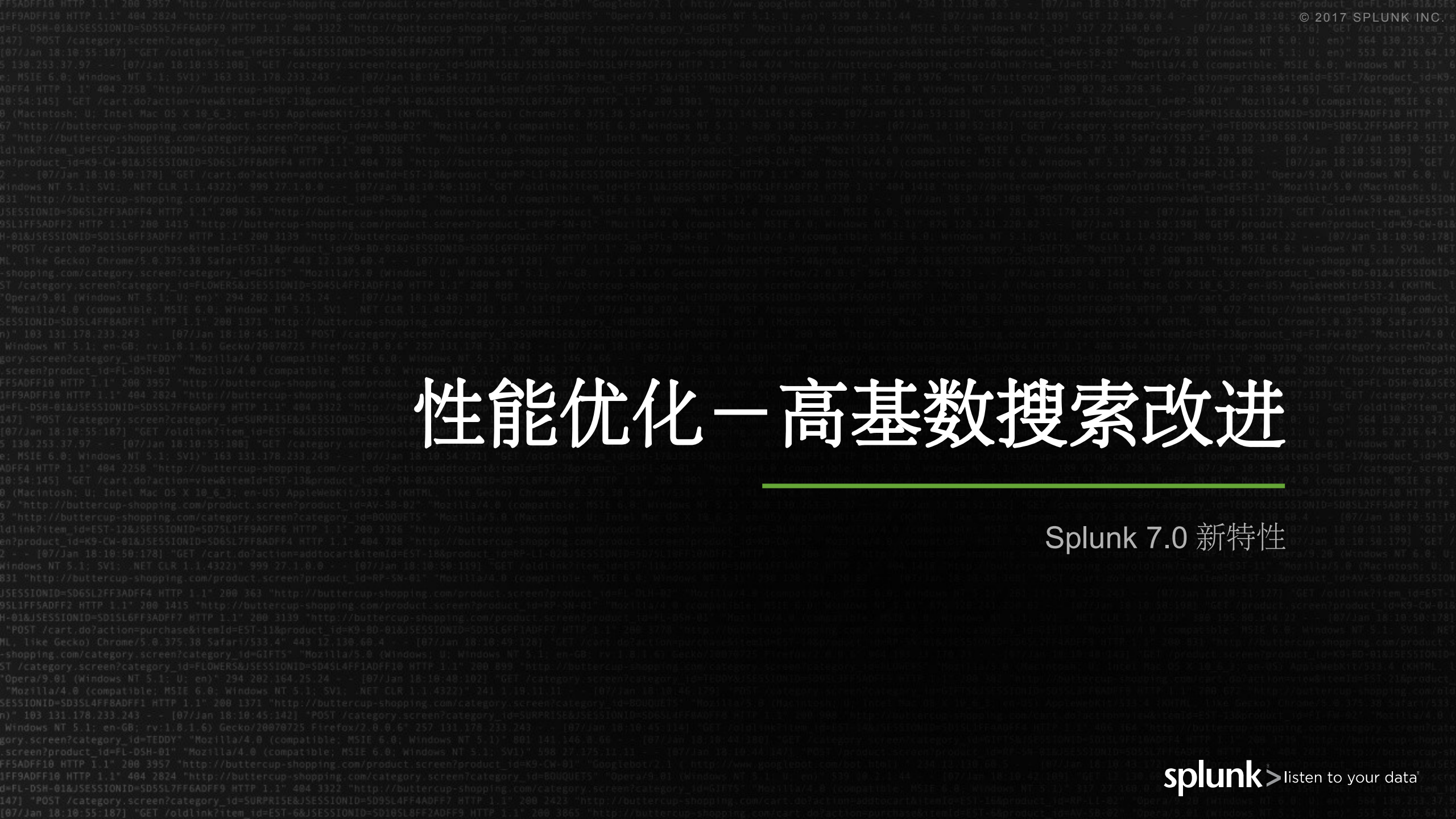
- 在加速历史数据的时候不能暂停，数据桶比较大时非常耗时
- 木桶效应：数据的不平衡导致低并发，最慢的 **indexer** 决定总的执行时间

► 解决方法

- 允许停止 / 继续加速数据桶，用 **acceleration.max_time** 控制
- 下一次加速从最新的数据桶开始，保证数据被加速的延时最低
- 如果有的进程提前加速完毕，允许其继续对新的数据继续进行加速 (设置 **acceleration.poll_buckets_until_maxtime=true**)

► 影响

- Splunk 7.0 加速比上个版本快两倍
- Splunk 7.0 加速延迟比上个版本减少 50 %
- 对重构加速索引的影响变小



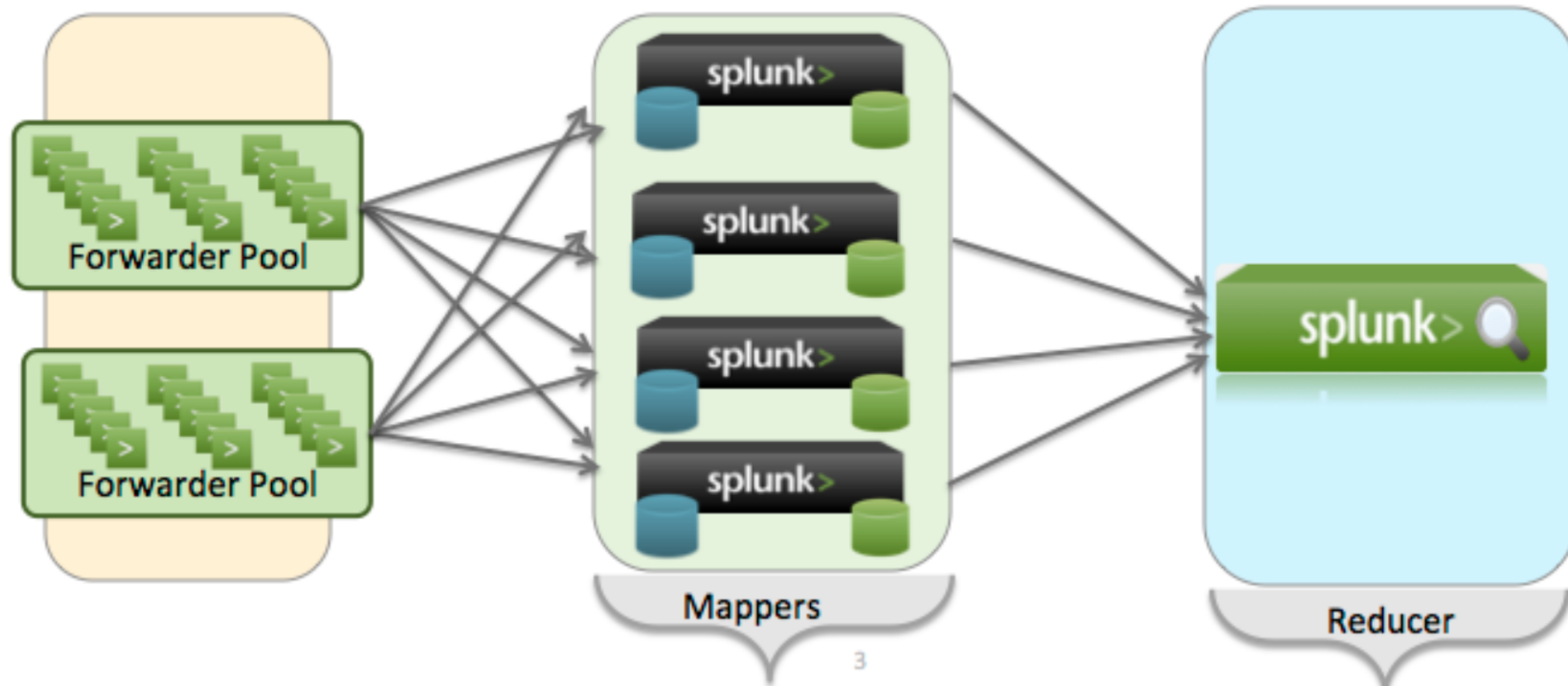
性能优化—高基数搜索改进

Splunk 7.0 新特性

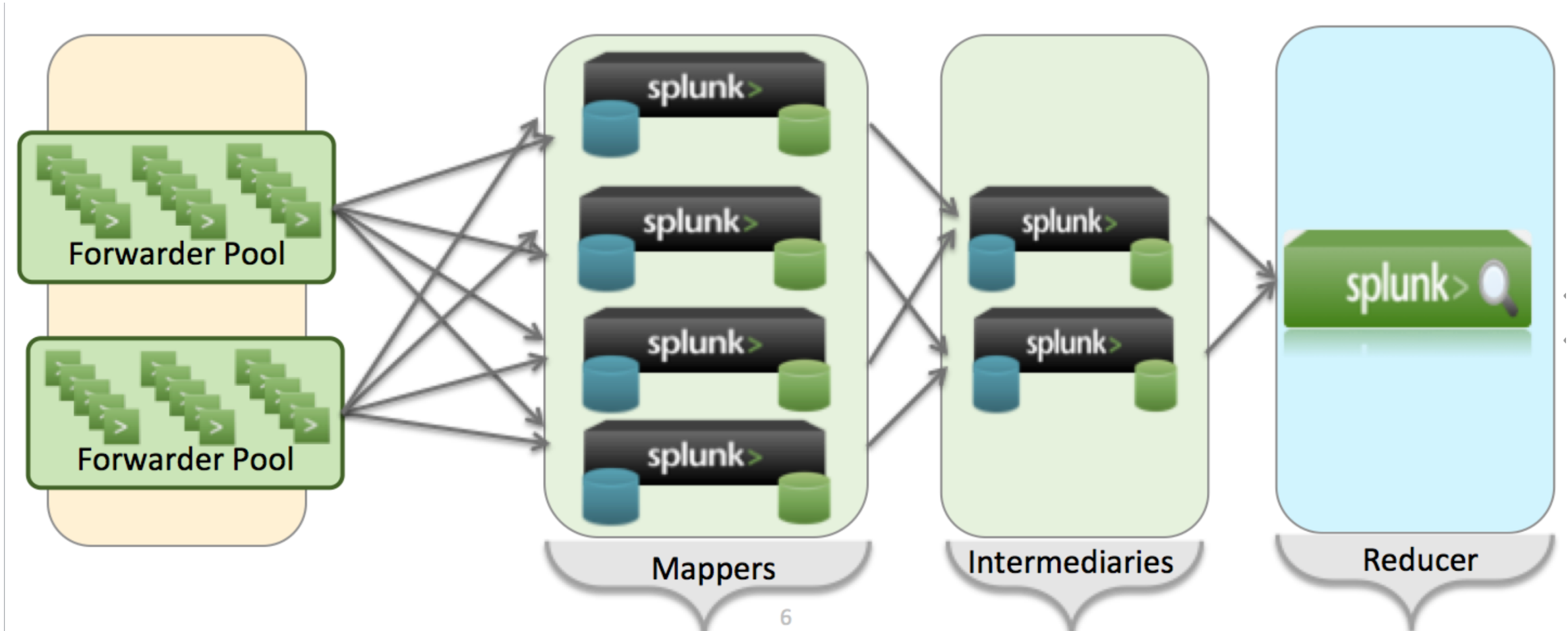
优化高基数 (Cardinality) 处理

- ▶ 如下搜索语句
 - `search tag=authentication | stats sum(bytes) by host`
- ▶ 搜索的性能跟 **host** 的数量密切相关

Parallel Reduce 之前



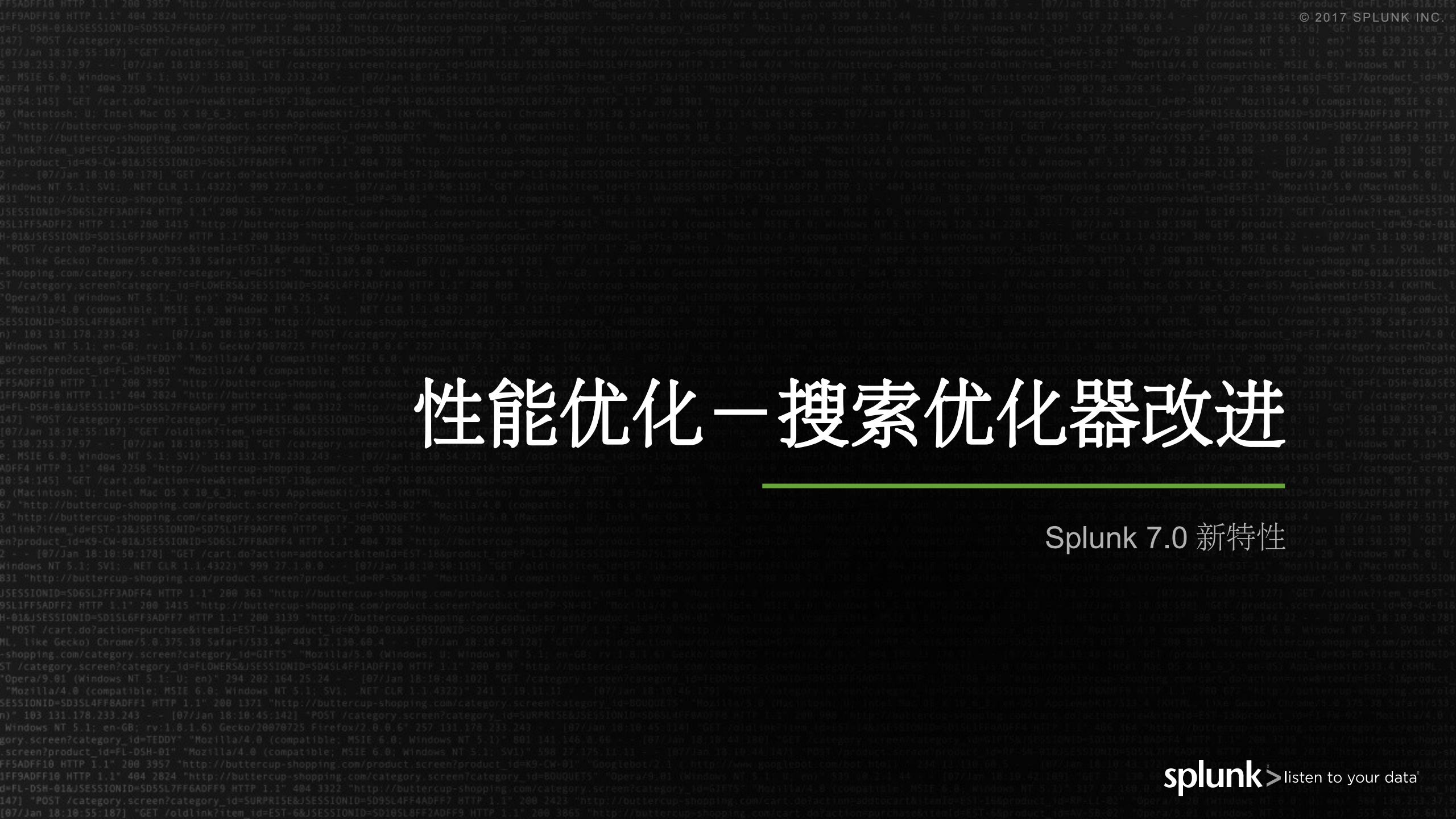
Parallel Reduce 之后



优化高基数 (Cardinality) 处理

使用 Parallel Reduce

- ▶ 如下搜索语句
 - search tag=authentication | stats sum(bytes) by host
- ▶ 搜索的性能跟 **host** 的数量密切相关
- ▶ Splunk 7.0 中部分支持
 - 启用设置
 - 在 **limits.conf** 中, 设置 **phased_execution=true**
 - 在搜索语句中加入 **| noop phase_mode=3**
 - 目前只支持 **stats**, **transaction** 和 **tstats**
- ▶ 下一个版本引入更多的提升



性能优化—搜索引擎改进

Splunk 7.0 新特性

搜索优化器

▶ 投射消除 (Projection Elimination)

- search ERROR | eval x=a*b | lookup users uid OUTPUT username | stats count by host
- search ERROR | stats count by host

▶ 断言拆分 (Predicate Splitting)

- | eval x=a+b | where x>10 and y<10
- | where y<10 | eval x=a+b | where x>10

▶ 合并 eval 命令

- | eval x=a+b | eval y=c+d
- | eval x=a+b, y=c+d

展望

指标存储

- 从日志中自动抽取指标数据
- 内部监控指标数据活动
- **TA** 支持

性能优化

- 4月中旬 北京 meetup 性能专场

