搜索性能改进

Splunk 7.0的新特性

2018.01.13

作者

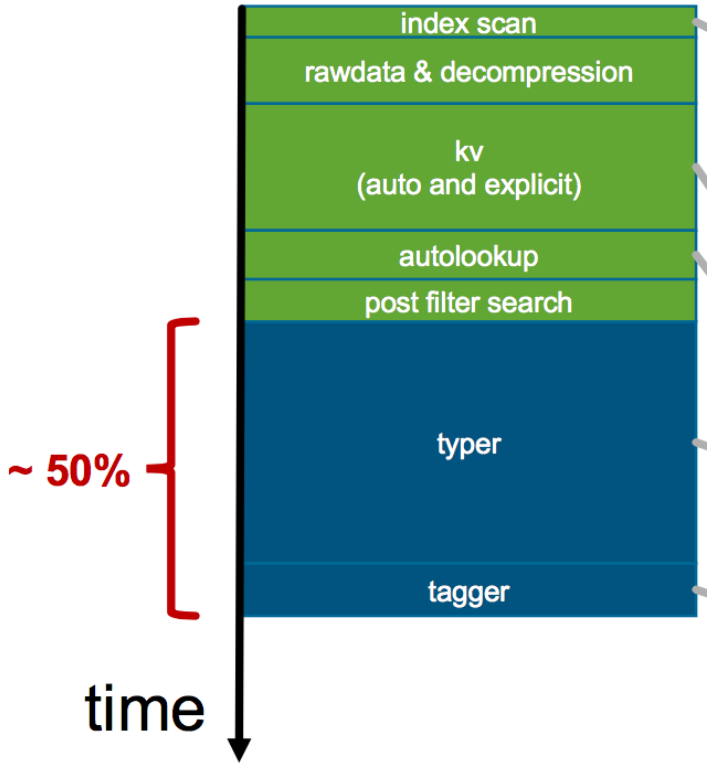
- Alex James - Senior Principal Product Manager (Search Technologies)
- Manan Brahmkshatriya - Principal QA Engineer

大纲

- 搜索语言改进
- 搜索优化器改进
- 数据模型加速改进

搜索执行时间分析

一个典型的安装了多个TA的Splunk环境



Duration (seconds)	Component	Invocations	Input count	Output count
0.01	command.fields	30	214,957	214,957
10.70	command.remotetl	30	214,957	-
67.83	command.search	60	214,957	429,914
4.30	command.search.index	191	-	-
3.49	command.search.filter	44	-	-
2.46	command.search.fieldalias	44	217,432	217,432
1.73	command.search.calcfields	44	217,432	217,432
0.28	command.search.expand_search	1	-	-
0.00	command.search.index.usec_1_8	1,384,938	-	-
0.00	command.search.index.usec_64_512	7	-	-
0.00	command.search.index.usec_8_64	1,408	-	-
24.04	command.search.typer	44	214,957	214,957
17.76	command.search.kv	44	-	-
8.94	command.search.lookups	44	217,432	217,432
3.90	command.search.tags	44	214,957	214,957
1.15	command.search.rawdata	44	-	-
0.00	command.search.summary	30	-	-
0.00	command.search.parse_directives	1	-	-

搜索指令 - DIRECTIVES

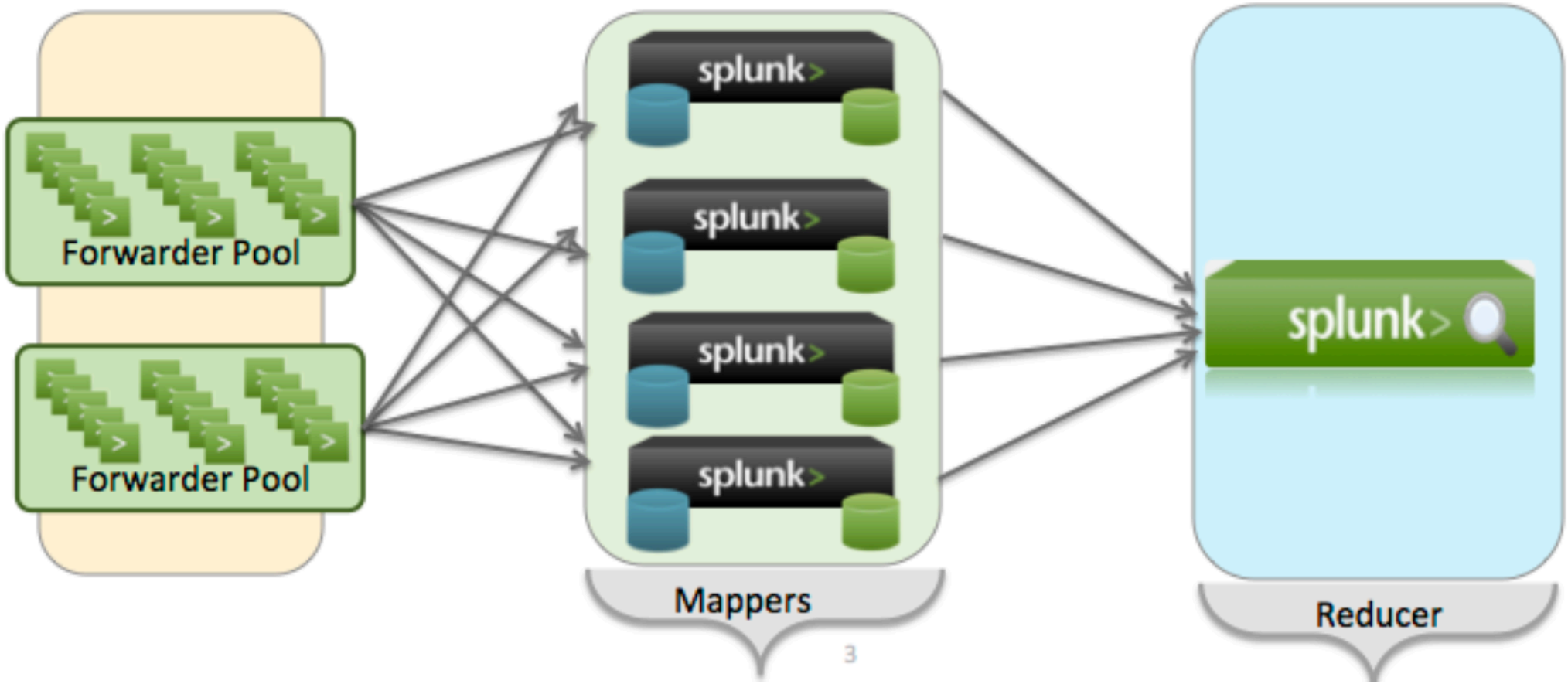
- 产生Tags和Eventtypes是很费时的
  - 搜索返回的每一个结果都会在所有的Tags和Eventtypes上做过滤
  - 当一个Splunk的环境里安装了多个TA，它可以占据超过50%的执行时间
- Splunk7.0提供一种新的方法来限定Tags(Eventtypes)
  - search 500 DIRECTIVES(REQUIRED_TAGS(tags="foo, bar"))
  - search 500 DIRECTIVES(REQUIRED_EVENTTYPES(eventtypes="alpha,omega"))
- 合并指令
  - search 500 DIRECTIVES(REQUIRED_EVENTTYPES(eventtypes="alpha,omega"),REQUIRED_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

优化高基数(Cardinality)处理

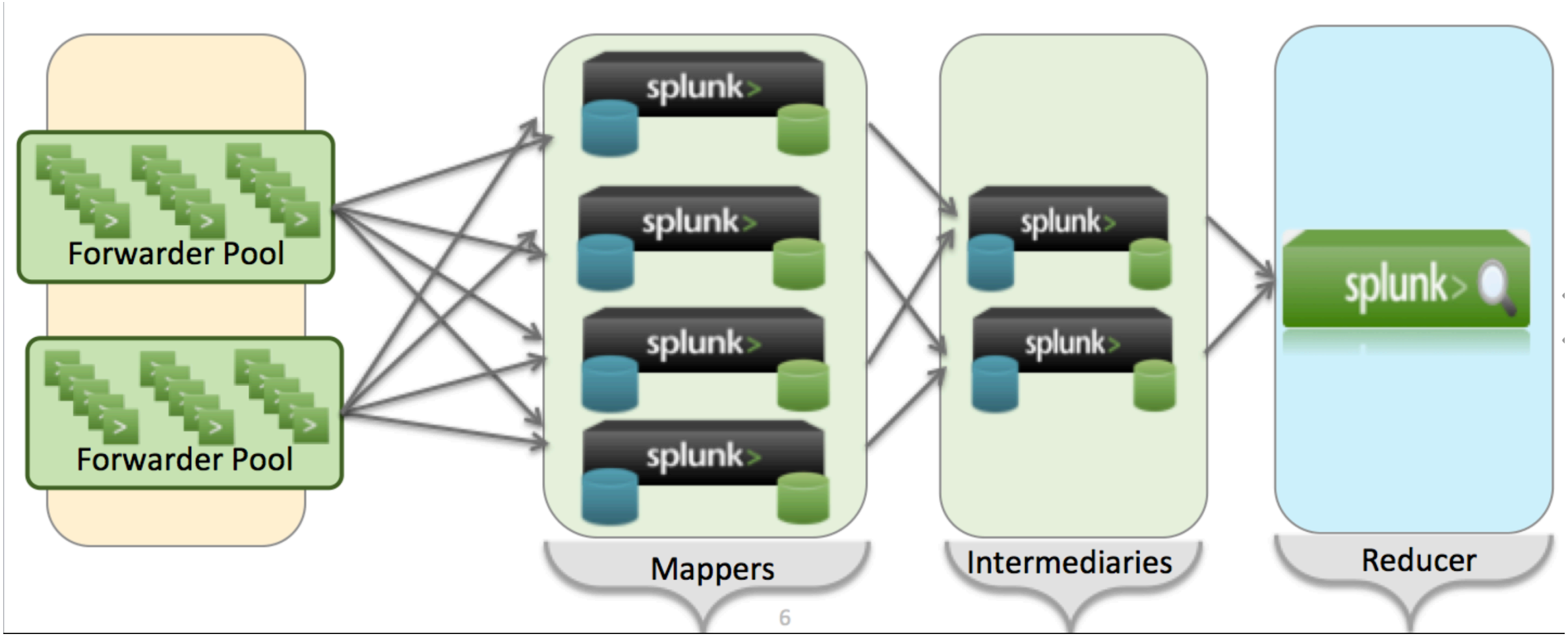
使用 Parallel Reduce

- 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
- 在stats之前隐式调用shuffle
  - search tag=authentication | **shuffle by host** | stats sum(bytes) by host
  - Reduce能并发做
- 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改进

Parallel Reduce之前



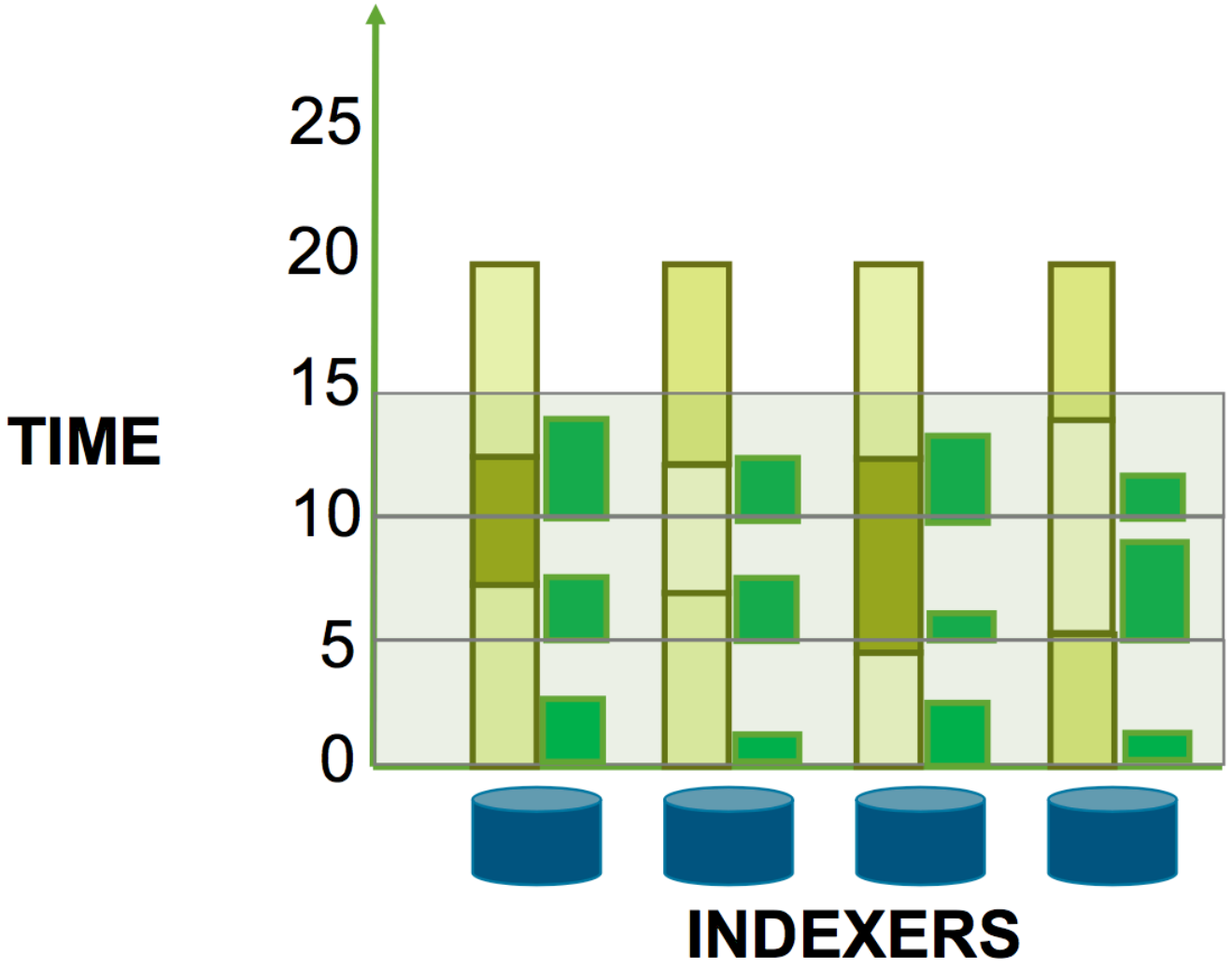
Parallel Reduce之后



Splunk 7.0新的搜索优化器

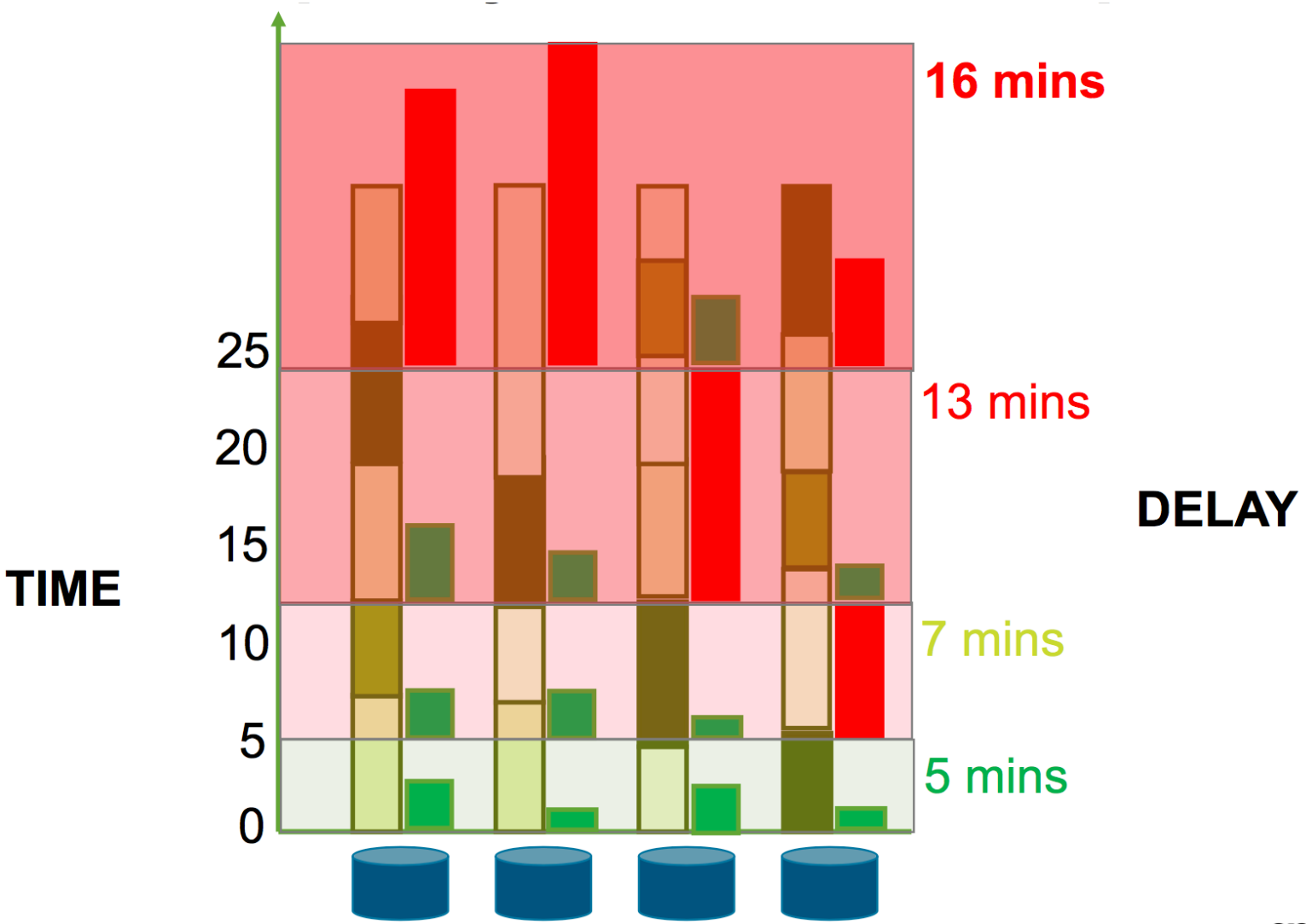
- Projection Elimination
  - search ERROR | eval x=a*b | lookup users uid OUTPUT username | stats count by host
  - search ERROR | stats count by host
- Predicate Splitting
  - | eval x=a+b | where x=10 and y=10
  - | where y=10 |eval x=a+b |where x=10
- Tag Elimination
  - search ERROR | where tag="Authentication" | stats count by host
  - search DIRECTIVES(REQUIRED_TAGS(tags="Authentication")) | where tag=Authentication | stats count by host
- Collapsing evals commands
  - | eval x=a+b | eval y=c+d
  - | eval x=a+b, y=c+d

数据模型加速(Data Model Acceleration) 如何工作



索引数据不一致引起的性能问题

Splunk 7.0之前



数据模型加速(Data Model Acceleration)

问题和解决方法

- Splunk 7.0之前
  - 在加速冷/热数据桶的时候不能暂停，一次做完或者失败，在加速大的数据桶时非常耗时
  - 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，最热的数据桶开始，保证数据被加速的延时最低
  - 在并发加速下，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下加速比上个版本快了两倍
  - 对一次性重建整个加速索引没有影响

关键点

1. Splunk 7.0搜索性能显著提高
2. 关键优化点
   - 新的指令DRRECTIVES
   - 优化高基数(Cardinality)处理
   - 搜索优化器的改进
   - Data Model Acceleration的改进

谢谢！