.conf18

splunk>

Turbo Charging the Elephant

Search Performance Optimization Techniques for Splunk Analytics for Hadoop

Holger Sesterhenn | Staff Sales Engineer

Raanan Dagan | Principal Architect

2018-08-30 | Orlando, FL

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Who we are

Holger Sesterhenn

- Staff Sales Engineer from Germany
- With Splunk for 6 years
- Focus on large accounts and complex architecture
- Loves craft beer
- Enjoys Marvel movies
- Pretends to do sports… sometimes

Raanan Dagan

- Principal Architect, Open Source
- Focused on open source technologies & integration
- 20+ years of experience building large scale data platforms
- Joined Splunk in 2012
- Avid soccer (football) player

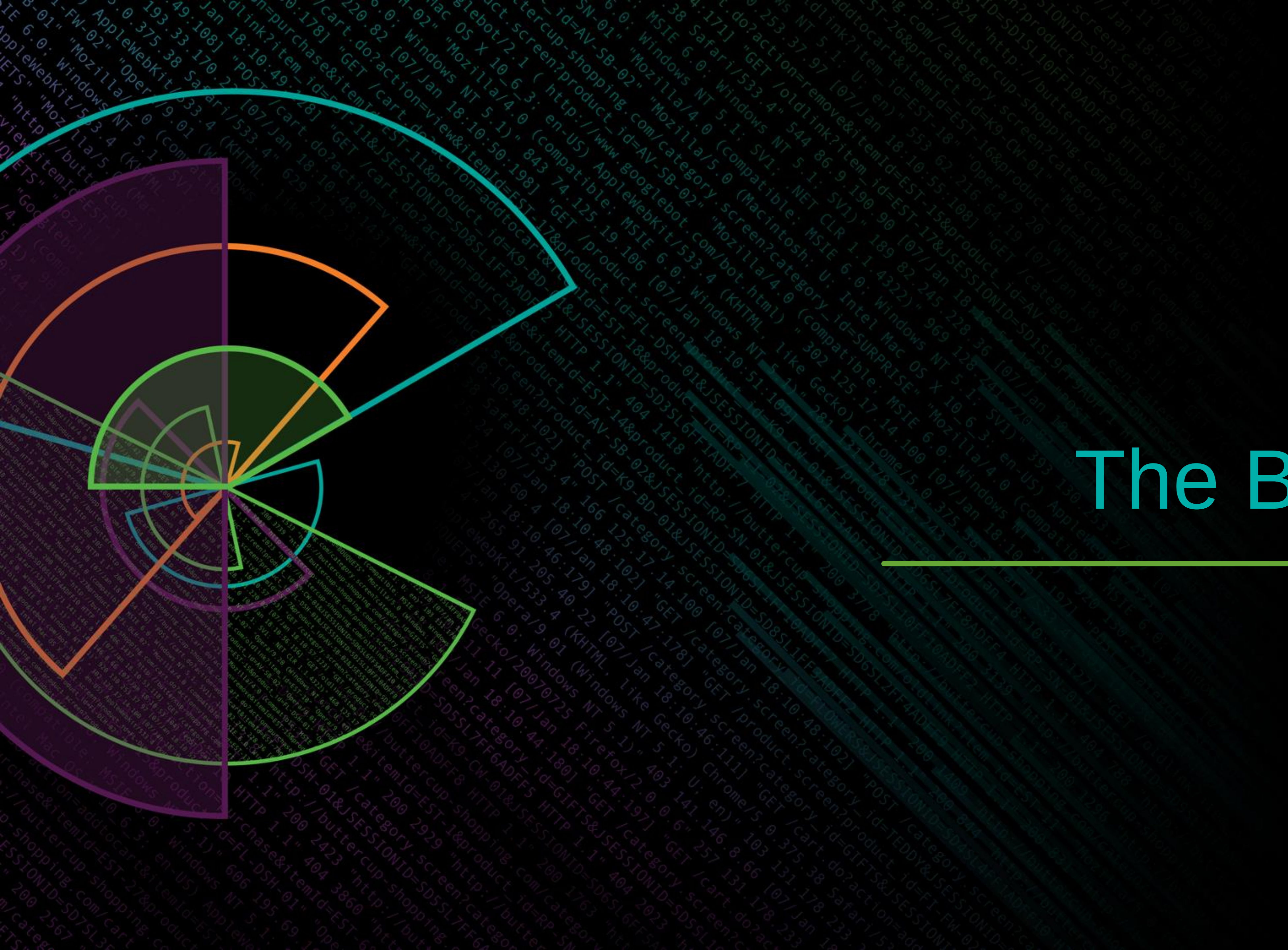
Splunk and Hadoop

What is slow and why it‘s different?

“Splunk Enterprise is optimized for time serialized data using an index –

Hadoop/HDFS/MR are for batch processing“

Don‘t mix the use cases!



The Basics

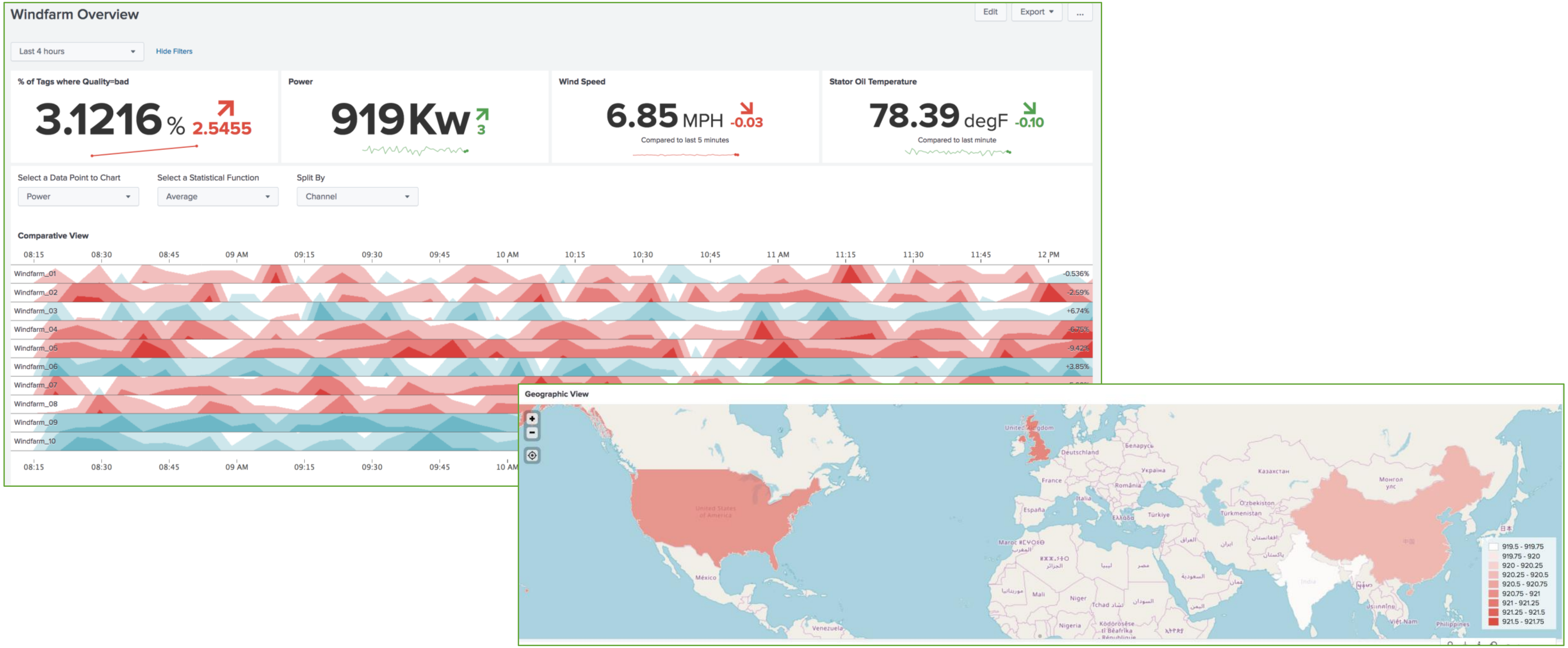
Splunk Analytics and Hadoop

What we are doing

- Main use case = Analyze Hadoop Data using Hadoop Processing (HDFS+MR)
  - It's just the search head… no Splunk Indexers anymore, but you can go hybrid
- Connect Splunk SH to Hadoop Cluster using a provider
  - You can connect multiple Hadoop Clusters to one Splunk SH
- Define a virtual index (VIX) for every data source you want to search
  - Usually you don't mix different sourcetypes in the same file/directory
- Schema on read is still used
  - `props.conf` and `transforms.conf` can be used to extract fields of interest

Use your SPL foo to search your data lake

UseCase: Windfarm



Windfarm Overview

Last 4 hours

Hide Filters

% of Tags where Quality=bad: 3.1216 % 2.5455

Power: 919 Kw 3

Wind Speed: 6.85 MPH -0.03 Compared to last 5 minutes

Stator Oil Temperature: 78.39 degF -0.10 Compared to last minute

Select a Data Point to Chart: Power

Select a Statistical Function: Average

Split By: Channel

Comparative View

Windfarm_01 -0.536%
Windfarm_02 -2.59%
Windfarm_03 +6.74%
Windfarm_04 -6.75%
Windfarm_05 -9.42%
Windfarm_06 +3.85%
Windfarm_07
Windfarm_08
Windfarm_09
Windfarm_10

Geographic View

919.5 - 919.75
919.75 - 920
920 - 920.25
920.25 - 920.5
920.5 - 920.75
920.75 - 921
921 - 921.25
921.25 - 921.5
921.5 - 921.75

Example Virtual Index

Connect a Hadoop HDFS cluster with a Splunk Analytics SearchHead

HDFS = /user/splunk/datalake/windfarm/20180824/09/windmill01/power.gz

```
[windfarm]
vix.provider = MyHadoopProvider
vix.input.1.path = /user/splunk/datalake/windfarm/*/*/${windmill}/...
vix.input.1.accept = \.gz$
vix.input.1.et.regex = .*?/datalake/windfarm/.*/(\d+)/(\d+)/.*?.gz
vix.input.1.et.format = yyyyMMddHH
vix.input.1.et.offset = 0
vix.input.1.lt.regex = .*?/datalake/windfarm/.*/(\d+)/(\d+)/.*?.gz
vix.input.1.lt.format = yyyyMMddHH
vix.input.1.lt.offset = 3600
```

http://docs.splunk.com/Documentation/Splunk/latest/HadoopAnalytics/Virtualindexes

Running a Splunk Analytics Search in Hadoop

Streaming, Hadoop MR and the like

1. `index=windfarm | head 1000`

   - A streaming search: just reading files from HDFS and stream them back to the splunkd process

2. `index=windfarm | stats count by windmill` (smart mode)

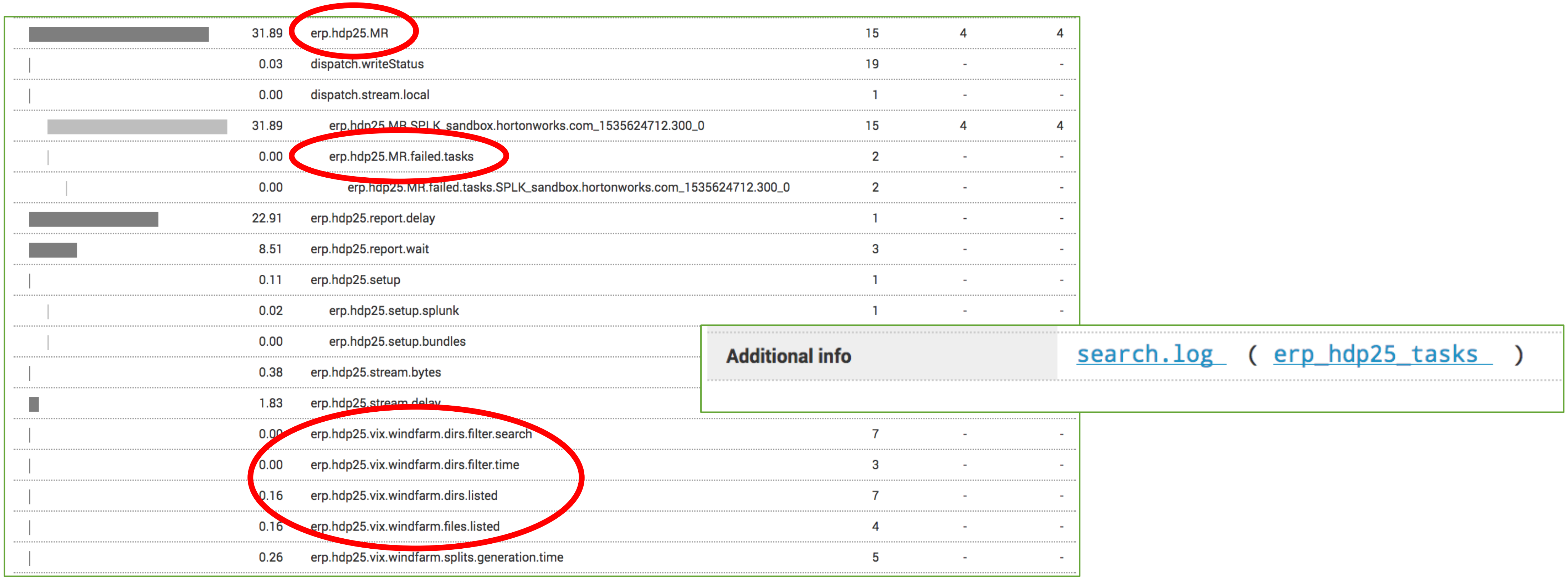
   - Read some files directly from HDFS - return results immediately / event timeline updates
   - Start MR jobs to search the majority of files (higher increments of events processed)

3. `index=windfarm | stats count by windmill` (verbose mode)

   - Don‘t start MR jobs at all! ONLY streaming!

Verify a MapReduce job is running

Screenshot of JobInspector/Logfile



31.89	erp.hdp25.MR	15	4	4
0.03	dispatch.writeStatus	19	-	-
0.00	dispatch.stream.local	1	-	-
31.89	erp.hdp25.MR.SPLK_sandbox.hortonworks.com_1535624712.300_0	15	4	4
0.00	erp.hdp25.MR.failed.tasks	2	-	-
0.00	erp.hdp25.MR.failed.tasks.SPLK_sandbox.hortonworks.com_1535624712.300_0	2	-	-
22.91	erp.hdp25.report.delay	1	-	-
8.51	erp.hdp25.report.wait	3	-	-
0.11	erp.hdp25.setup	1	-	-
0.02	erp.hdp25.setup.splunk	1	-	-
0.00	erp.hdp25.setup.bundles			
0.38	erp.hdp25.stream.bytes			
1.83	erp.hdp25.stream.delay			
0.00	erp.hdp25.vix.windfarm.dirs.filter.search	7	-	-
0.00	erp.hdp25.vix.windfarm.dirs.filter.time	3	-	-
0.16	erp.hdp25.vix.windfarm.dirs.listed	7	-	-
0.16	erp.hdp25.vix.windfarm.files.listed	4	-	-
0.26	erp.hdp25.vix.windfarm.splits.generation.time	5	-	-

Additional info search.log (erp_hdp25_tasks)

```
08-30-2018 10:25:18.413 INFO ERP.hdp25 - SplunkBaseMapper - using class=com.splunk.mr.input.SplunkLineRecordReader
to process split=/user/root/data/windfarm/opc/20180804/12/Power/windfarm_03-20180804_12-Power.opc.txt.gz:0+24275
```

Behind the Scenes

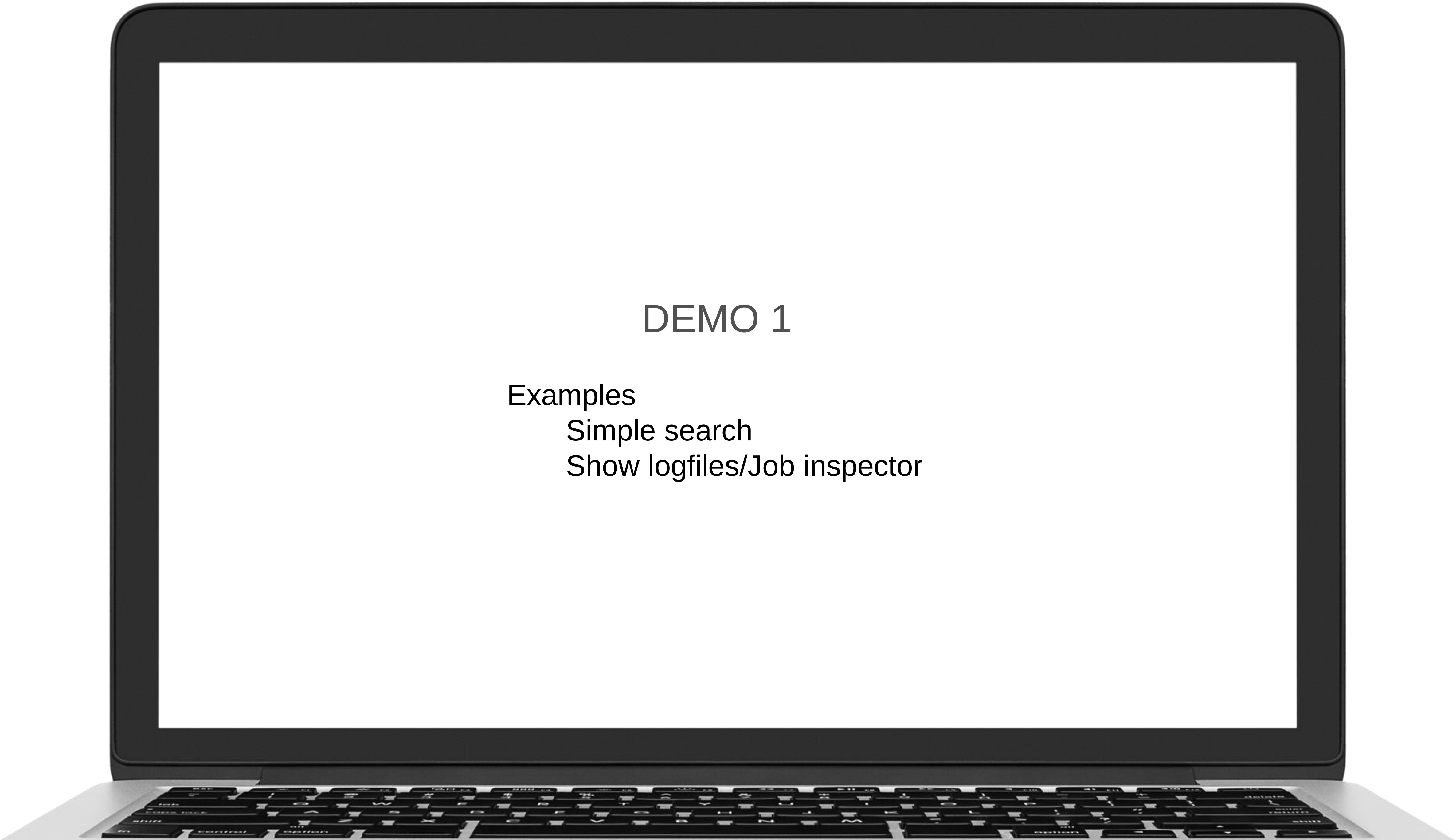
1. Splunk SH is creating search bundles for every Hadoop DataNode/TaskTracker

2. SplunkD process on every DataNode/TaskTracker either streams data or gets results from MapReduce jobs

3. SplunkD is processing the data (schema on read) and filters
   - Lookups are applied on the TaskTracker!

4. Data is sent back to Splunk SH (Hadoop Analytics)

This is a full event scan because there is no index (TSIDX) involved -
a lot of work to do if you just search for a “needle in a haystack” (AKA IP address e.g.)



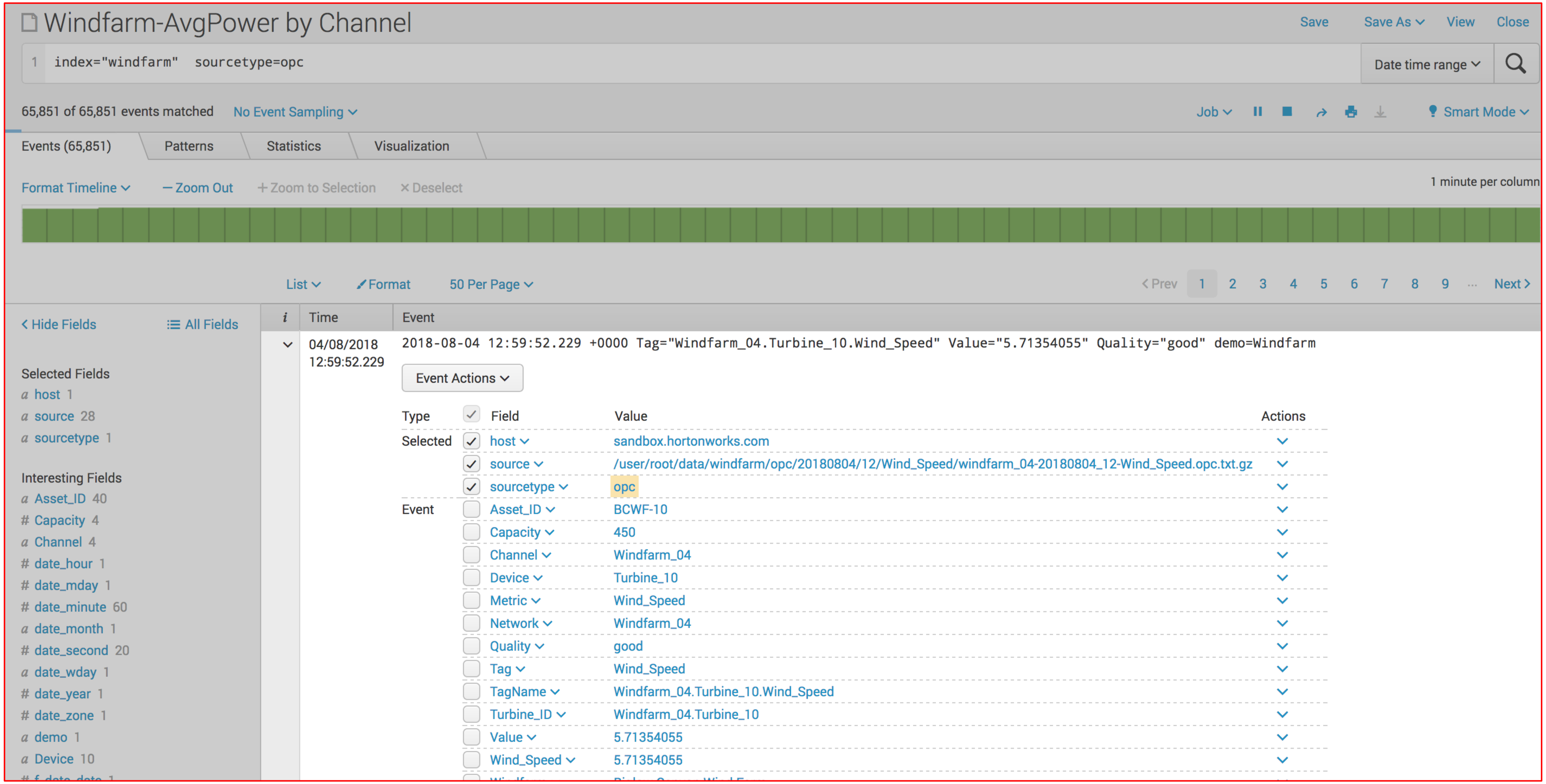
DEMO 1

Examples

- Simple search
- Show logfiles/Job inspector

Backup Screenshot

Simple search with lookup data



Windfarm-AvgPower by Channel

```
index="windfarm"  sourcetype=opc
```

65,851 of 65,851 events matched   No Event Sampling

Events (65,851)   Patterns   Statistics   Visualization

1 minute per column

i	Time	Event
	04/08/2018 12:59:52.229	2018-08-04 12:59:52.229 +0000 Tag="Windfarm_04.Turbine_10.Wind_Speed" Value="5.71354055" Quality="good" demo=Windfarm

Type	✓	Field	Value	Actions
Selected	☑	host	sandbox.hortonworks.com	
	☑	source	/user/root/data/windfarm/opc/20180804/12/Wind_Speed/windfarm_04-20180804_12-Wind_Speed.opc.txt.gz	
	☑	sourcetype	opc	
Event	□	Asset_ID	BCWF-10	
	□	Capacity	450	
	□	Channel	Windfarm_04	
	□	Device	Turbine_10	
	□	Metric	Wind_Speed	
	□	Network	Windfarm_04	
	□	Quality	good	
	□	Tag	Wind_Speed	
	□	TagName	Windfarm_04.Turbine_10.Wind_Speed	
	□	Turbine_ID	Windfarm_04.Turbine_10	
	□	Value	5.71354055	
	□	Wind_Speed	5.71354055	

Selected Fields

	Field	Count
a	host	1
a	source	28
a	sourcetype	1

Interesting Fields

	Field	Count
a	Asset_ID	40
#	Capacity	4
a	Channel	4
#	date_hour	1
#	date_mday	1
#	date_minute	60
a	date_month	1
#	date_second	20
a	date_wday	1
#	date_year	1
#	date_zone	1
a	demo	1
a	Device	10

Backup Screenshot

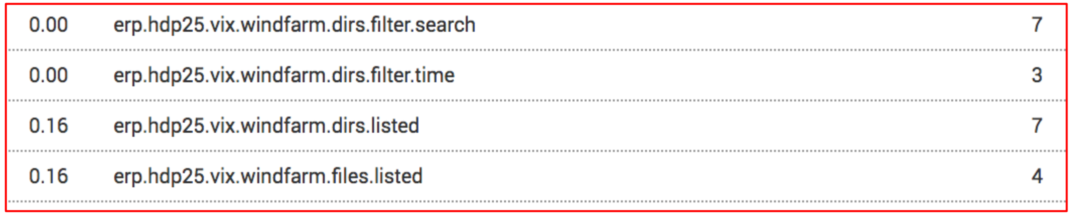
Loglines to show partition pruning

```
Search: index="windfarm"  sourcetype=opc f_tag="Power"
```

```
08-30-2018 10:49:55.384 DEBUG ERP.hdp25 - VirtualIndex - Updating source in search context to a
dir=/user/root/data/windfarm/opc/20180804/12/Power/
08-30-2018 10:49:55.384 DEBUG ERP.hdp25 - VirtualIndex - Dir meets the search criteria. Will consider it,
path=hdfs://172.17.0.1:8020/user/root/data/windfarm/opc/20180804/12/Power
08-30-2018 10:49:55.384 DEBUG ERP.hdp25 - VirtualIndex - Dir meets time heuristic
path=hdfs://172.17.0.1:8020/user/root/data/windfarm/opc/20180804/12/Power, search.et=1533384000, search.lt=1533387600,
file.et=1533384000, file.lt=1533387600, file.mtime=1534341390
```

```
08-30-2018 10:49:55.384 DEBUG ERP.hdp25 - VirtualIndex - Updating source in search context to a
dir=/user/root/data/windfarm/opc/20180804/12/Wind_Speed/
08-30-2018 10:49:55.384 DEBUG ERP.hdp25 - VirtualIndex - Dir does not meet the search criteria. Will not
consider it, path=hdfs://172.17.0.1:8020/user/root/data/windfarm/opc/20180804/12/Wind_Speed
```

```
08-30-2018 10:49:55.469 DEBUG ERP.hdp25 - VirtualIndex - Dir meets the search criteria.
Will consider it, path=hdfs://172.17.0.1:8020/user/root/data/windfarm/opc/20180804/10
08-30-2018 10:49:55.469 DEBUG ERP.hdp25 - VirtualIndex - Dir does not satisfy time
heuristic, path=hdfs://172.17.0.1:8020/user/root/data/windfarm/opc/20180804/10,
search.et=1533384000, search.lt=1533387600, file.et=1533376800, file.lt=1533380400,
file.mtime=1534341389
```



0.00	erp.hdp25.vix.windfarm.dirs.filter.search	7
0.00	erp.hdp25.vix.windfarm.dirs.filter.time	3
0.16	erp.hdp25.vix.windfarm.dirs.listed	7
0.16	erp.hdp25.vix.windfarm.files.listed	4

Best Practices - Part 1 -

Make sure the directory structure is useful

This is BAD

- /datalake/user/dir/<allfiles>...

This is GOOD (use the time picker to prune directories)

- /datalake/windfarm/opc/**20180801/0900**/<somefiles>....
- /datalake/windfarm/opc/**20180802/1000**/<otherfiles>....

This is BETTER (automatic field extraction!)

- /datalake/windfarm/${sourcetype}/**20180801/0900**/**metric=power**/<fewer files>...
- /datalake/windfarm/${sourcetype}/**20180801/1000**/**metric=wind_speed**/<fewer files>...

Reduce the amount of files scanned/read from HDFS

Structure by directory not by filename!

http://docs.splunk.com/Documentation/Splunk/latest/HadoopAnalytics/Setupvirtualindexes

Get results faster

Want your dashboards fast? Cache is king

Overview of options

1. Splunk (scheduled) saved search
   - https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Loadjob
   - http://docs.splunk.com/Documentation/Splunk/latest/Report/Schedulereports

2. Splunk summary index
   - Store the results of a search in Splunk Enterprise
   - http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Usesummaryindexing

3. Hadoop Analytics Report Acceleration
   - http://docs.splunk.com/Documentation/Splunk/latest/HadoopAnalytics/Workwithreportacceleration

4. Datamodel Acceleration, not just nice looking..
   - http://docs.splunk.com/Documentation/Splunk/latest/HadoopAnalytics/Datamodelacceleration

Hadoop Analytics Report Acceleration

Some more details

- You need a transforming search
- Don‘t work in verbose mode
- Store the results in HDFS
  - hdfs:///user/root/splunkmr702/cache/windfarm/d5b3fea992e7a90fabd20e71e2bf269c/_no_id/compacts/78967737-5757-44e9-a8f2-e7d258e8b97f
- Files are stored in `vix.splunk.search.cache.path`
- Works like Splunk Enterprise Report Acceleration

http://docs.splunk.com/Documentation/Splunk/latest/HadoopAnalytics/Configurereportacceleration

Hadoop Analytics Data Model Acceleration

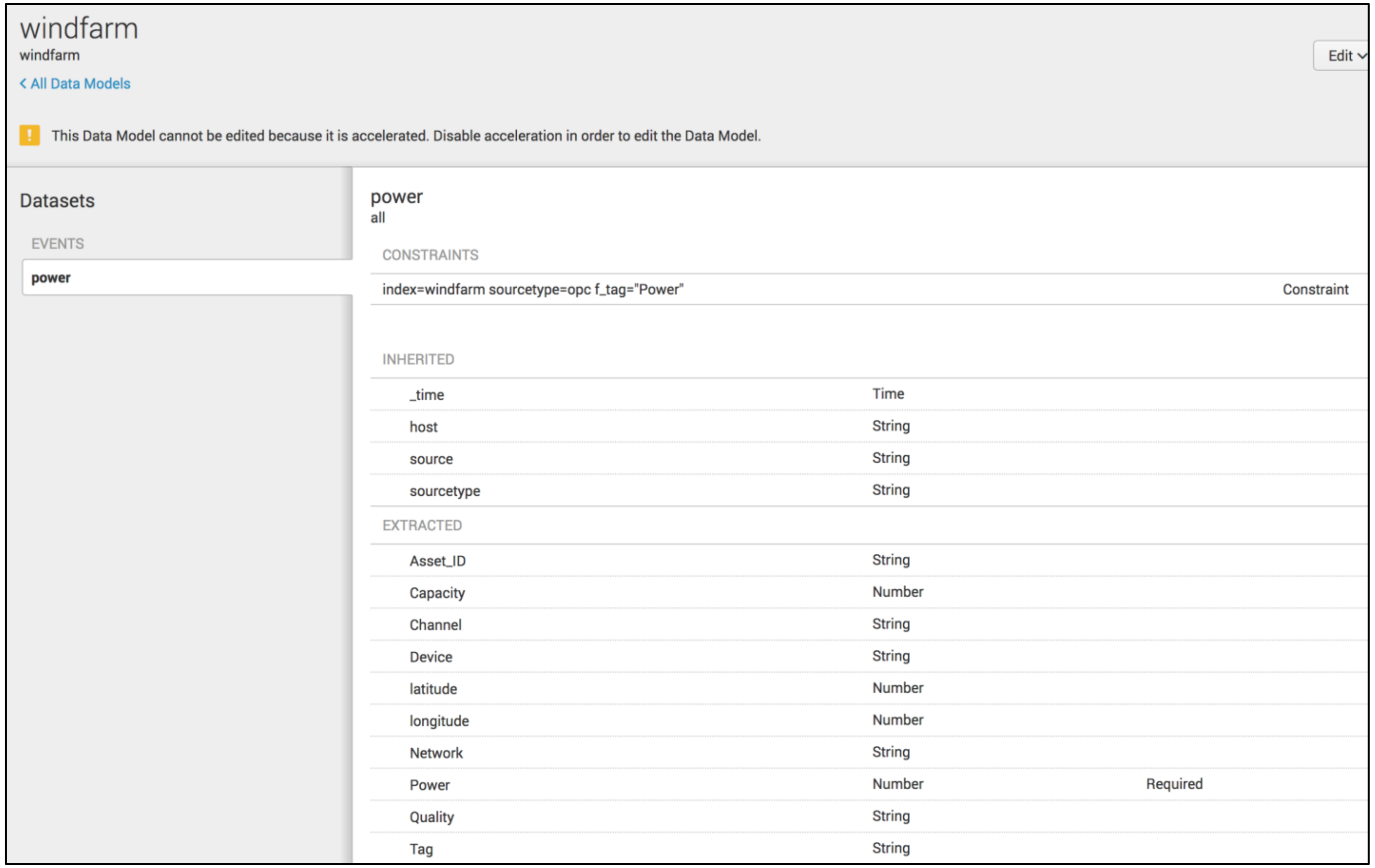
Some more details

- Configure a Splunk Enterprise Data Model
  - The constraint is using a VIX!
- Switch on accleleration
  - Mapreduce jos are running on a fixed schedule
  - Results are stored in ORC or Parquet file format
- Information about the DMA summary files stored in KV Store!
- Actual DMA files are stored in HDFS
- You can use „|tstats“ to search
  - http://docs.splunk.com/Documentation/Splunk/latest/HadoopAnalytics/Configuredatamodelacceleration

Hadoop Analytics DMA does not use TSIDX files!

The Windfarm Data Model

- Take fields from the lookup
- No need to do a lookup on TaskTracker anymore
- Store summary in HDFS structure
- TSTATS will run MR jobs on pre-computed summaries



windfarm

windfarm

< All Data Models

! This Data Model cannot be edited because it is accelerated. Disable acceleration in order to edit the Data Model.

Datasets

EVENTS

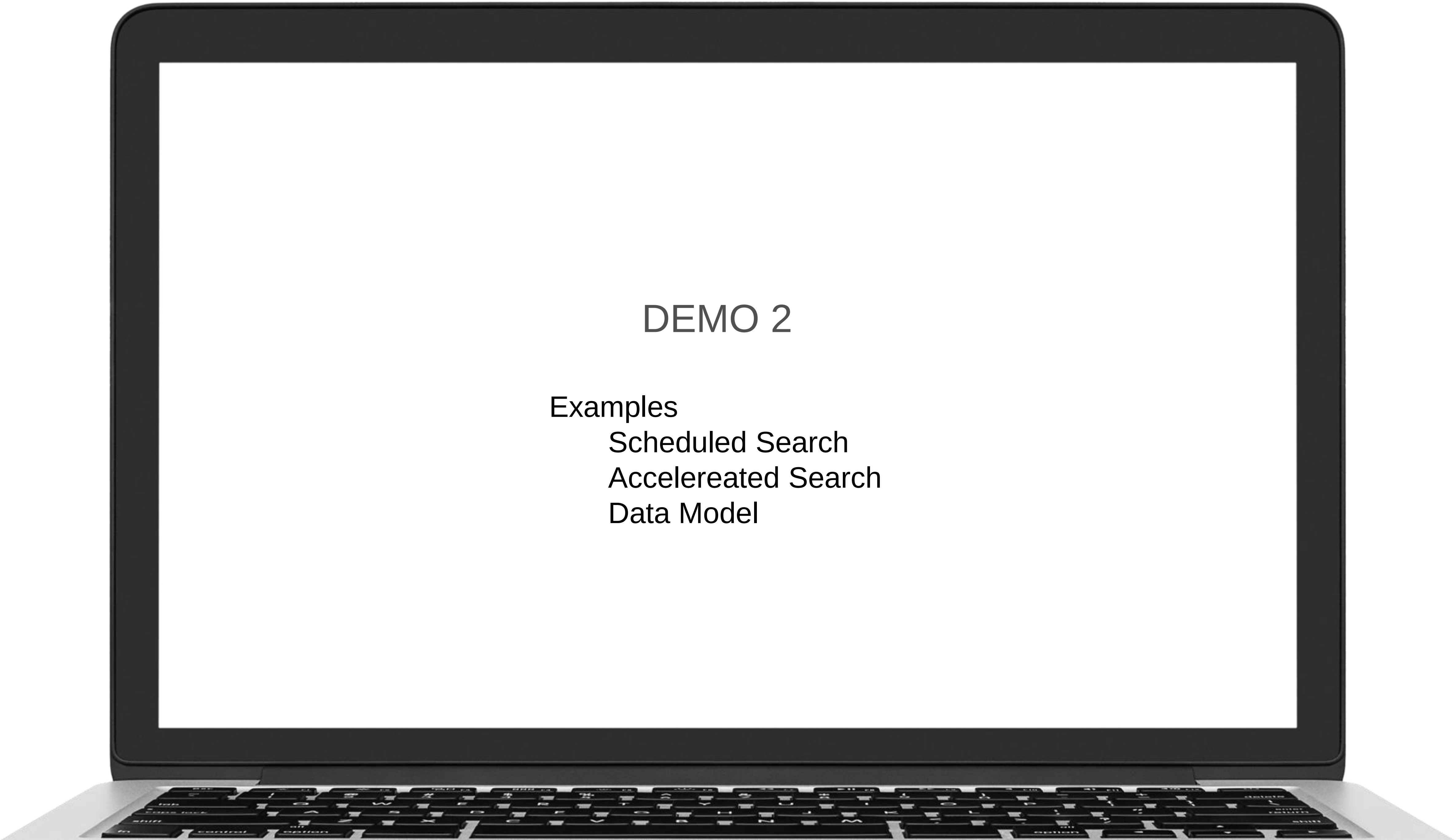
power

power

all

CONSTRAINTS		
index=windfarm sourcetype=opc f_tag="Power"		Constraint
INHERITED		
_time	Time	
host	String	
source	String	
sourcetype	String	
EXTRACTED		
Asset_ID	String	
Capacity	Number	
Channel	String	
Device	String	
latitude	Number	
longitude	Number	
Network	String	
Power	Number	Required
Quality	String	
Tag	String	

```
hdfs://localhost:8020/user/root/splunkmr702/datamodel/6026C1EB-B03C-405E-92F4-
7EB40D25D0F0_DM_demo_hadoop_windfarm_windfarm/windfarm
```



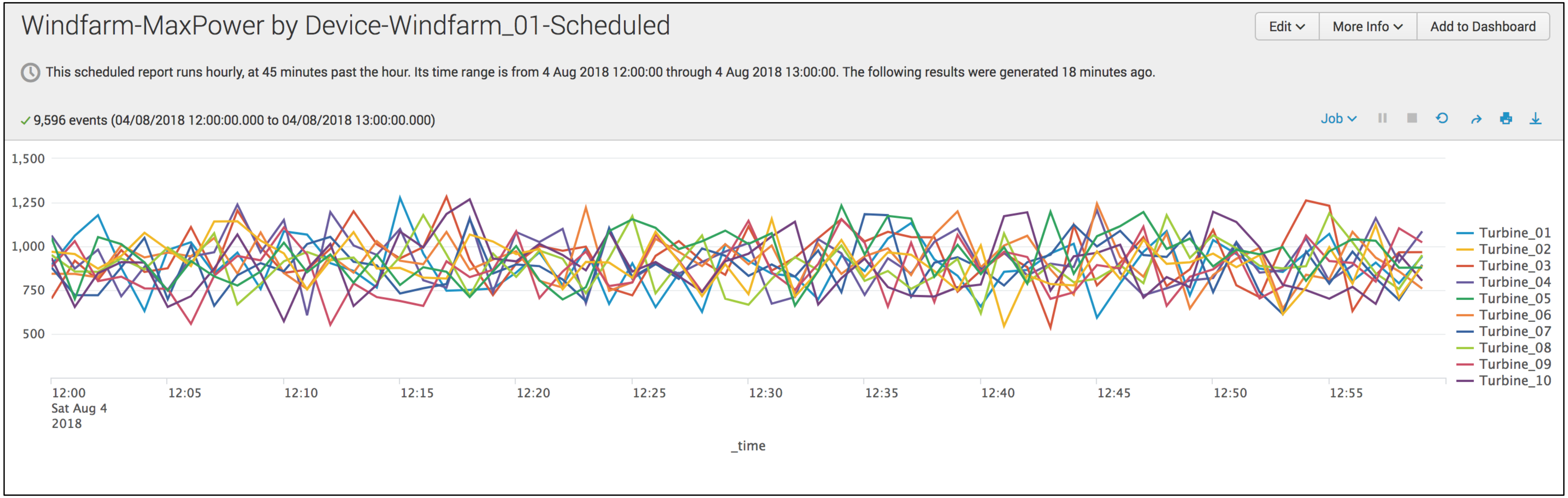
DEMO 2

Examples

- Scheduled Search
- Accelereated Search
- Data Model

Backup Screenshots

Scheduled Search



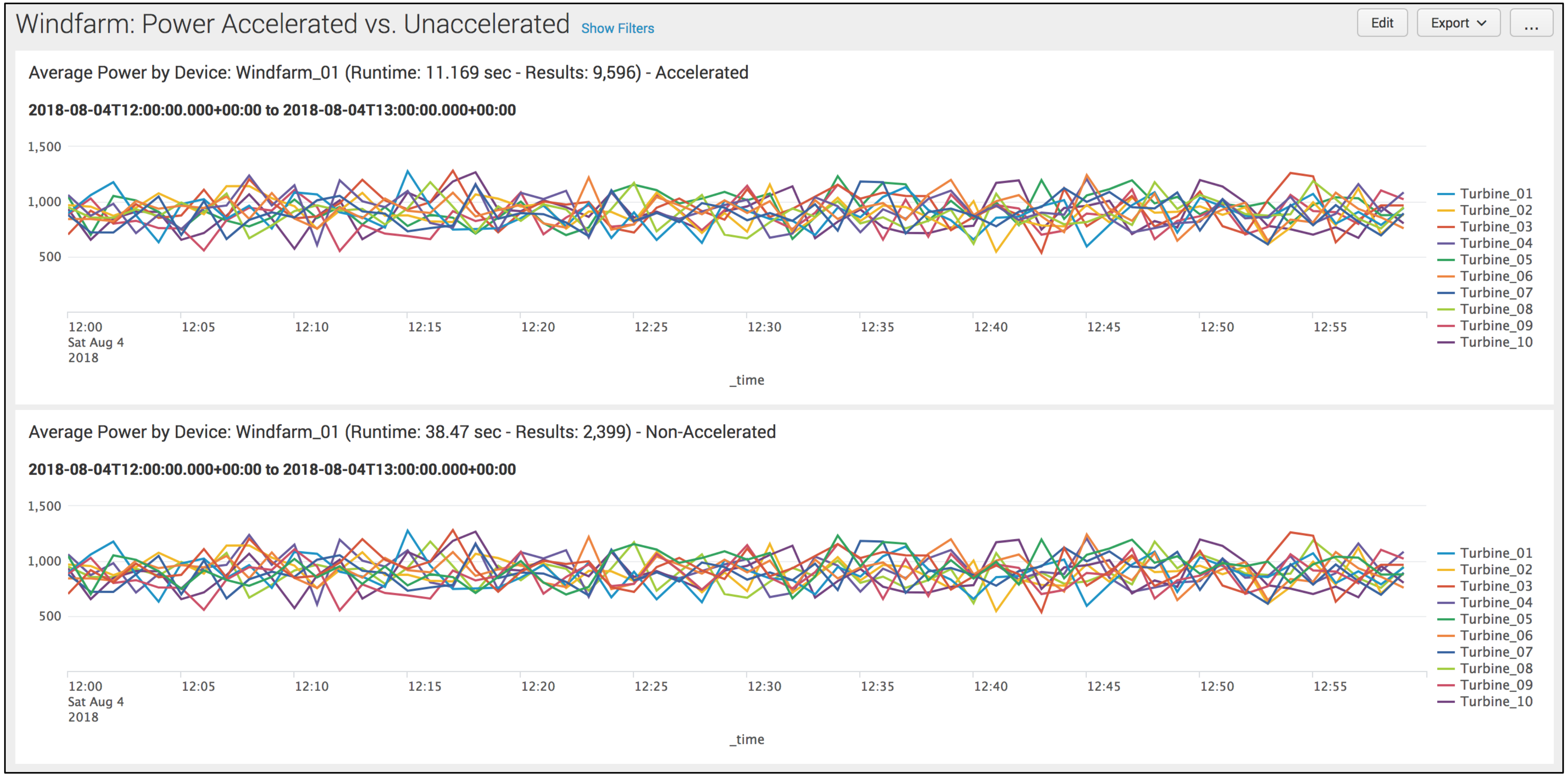
Windfarm-MaxPower by Device-Windfarm_01-Scheduled

This scheduled report runs hourly, at 45 minutes past the hour. Its time range is from 4 Aug 2018 12:00:00 through 4 Aug 2018 13:00:00. The following results were generated 18 minutes ago.

✓ 9,596 events (04/08/2018 12:00:00.000 to 04/08/2018 13:00:00.000)

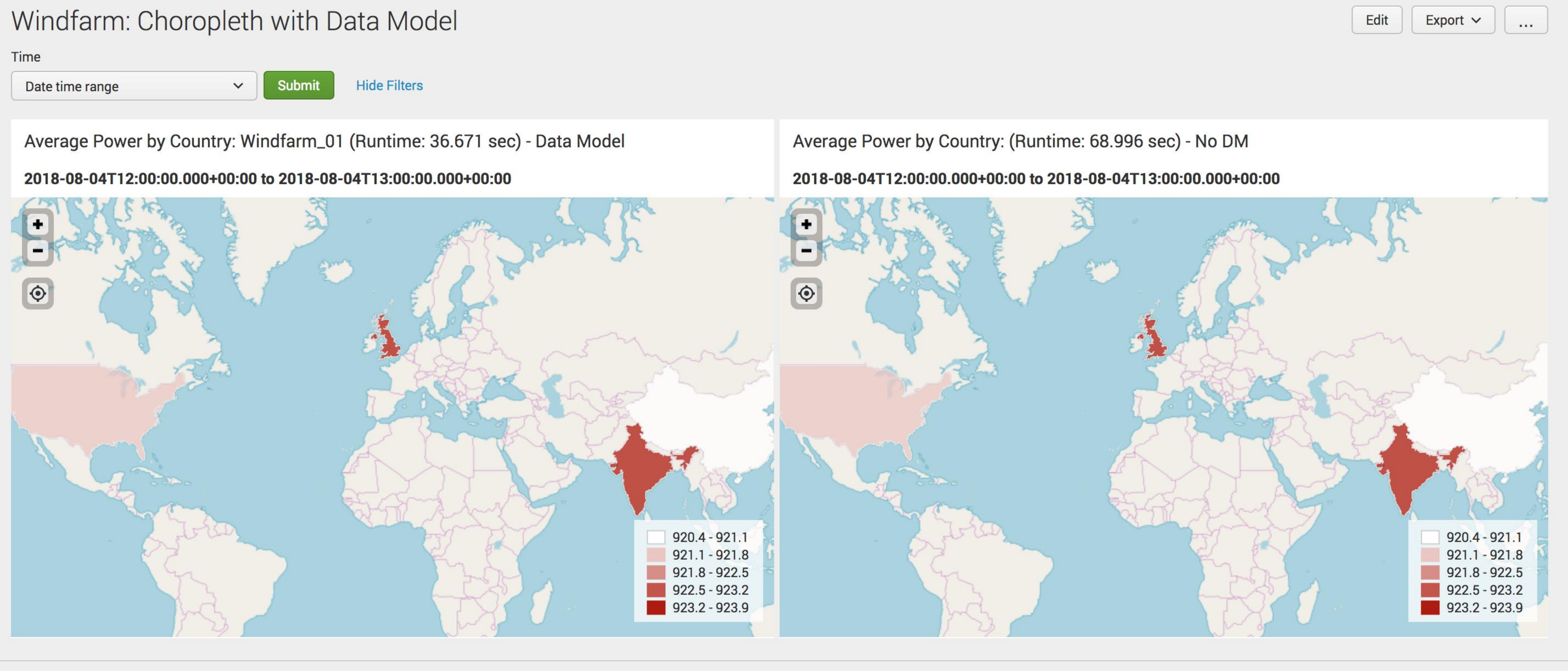
Backup Screenshots

Accelerated vs. Non-Accelerated Dashboard Panel



Backup Screenshots

Choropleth Example with Data Model



Windfarm: Choropleth with Data Model

Time: Date time range

Average Power by Country: Windfarm_01 (Runtime: 36.671 sec) - Data Model

2018-08-04T12:00:00.000+00:00 to 2018-08-04T13:00:00.000+00:00

Average Power by Country: (Runtime: 68.996 sec) - No DM

2018-08-04T12:00:00.000+00:00 to 2018-08-04T13:00:00.000+00:00

Best Practices - Part 2 -

Choose the right method for your use case

- Summary Indexing and Saved Searches store data on the SH!
  - Fast but not flexible
- Report Acceleration stores data on HDFS
  - Enough storage available
  - Not Flexible (only similar searches are accelerated)
  - Quite fast because just streaming no MR jobs
- Data Model Acceleration stores data on HDFS but creates summary files per original data file and spawn MR jobs
  - More flexible but slower than Report Acceleration
  - Remember, no TSIDX, no Random Access

What if the elephant burbs?

How to troubleshot if something goes wrong

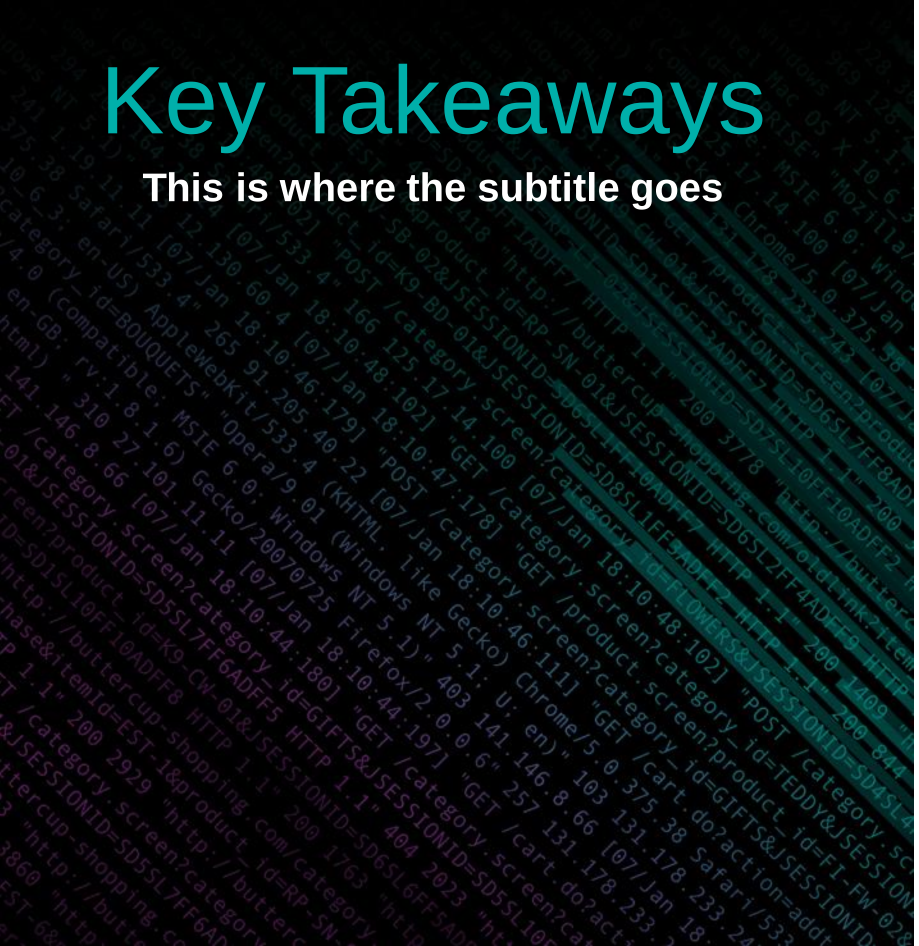
Troubleshooting Splunk Analytics for Hadoop

- Open the JobInspector first! -> search.log (maybe create an input?)
- Switch on debugging: `vix.splunk.search.debug=1` (provider)
- Doublecheck the provider settings (ports mixed?)
- Check: does a simple search works? HDFS streaming
  - `index=hadoop|head 10`
- Hadoop resource manager web page checked ("All Applications")?
  - Ressource Manager runs usually on <RM-IP>:8088/cluster
- Monitor the YARN logs
  - https://www.splunk.com/blog/2014/05/14/hunkonhunk.html
- https://conf.splunk.com/session/2015/conf2015_RDagan_Splunk_BigData_HUNKPerformanceandTroubleshooting.pdf

For Reference

If you want to read more…

- http://docs.splunk.com/Documentation/Splunk/latest/HadoopAnalytics/Performancebestpractices
- http://docs.splunk.com/Documentation/Splunk/latest/HadoopAnalytics/TroubleshootSplunkAnalyticsforHadoop
- https://www.splunk.com/blog/2015/05/05/caching-hadoop-data-with-splunk-and-hunk.html

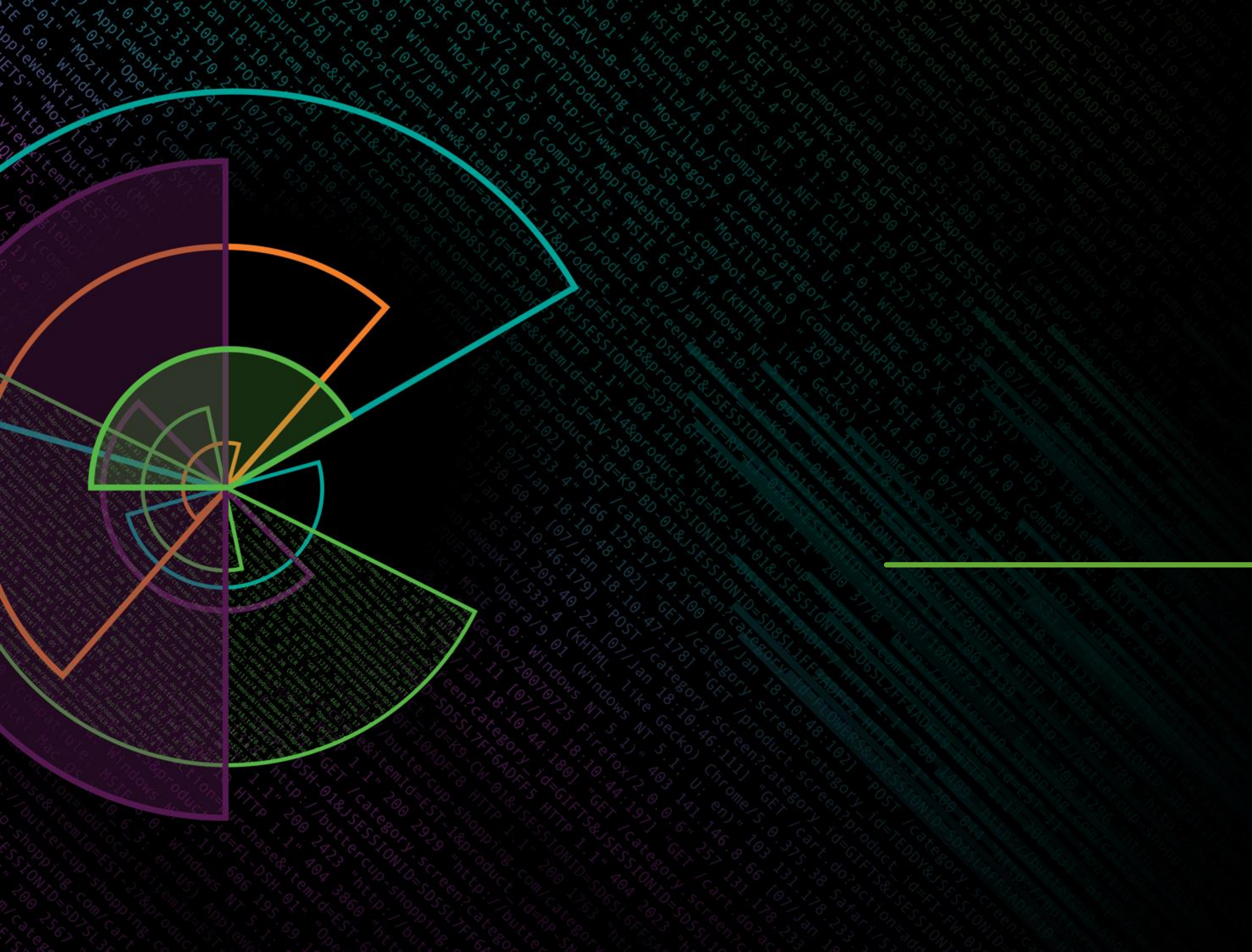


Key Takeaways

This is where the subtitle goes

1. Understand your use case
2. Structure your data in HDFS
3. Cache is KING!

Happy splunking!!!



Q&A

Thank You

Don't forget to rate this session
in the .conf18 mobile app

.conf18

splunk>