Experience with SPLUNK for archiving and visualisation of operational data in ATLAS TDAQ system

To cite this article: A Kazarov *et al* 2018 *J. Phys.: Conf. Ser.* **1085** 032052

Experience with SPLUNK for archiving and visualisation of operational data in ATLAS TDAQ system

A Kazarov[1], **G Avolio**[2], **A Chitan**[3] **and M Mineev**[4]

[1]NRC "Kurchatov Institute" - PNPI, St. Petersburg, Russian Federation
[2]CERN, Geneva, Switzerland
[3]National Institute of Physics and Nuclear Engineering, Bucharest, Romania
[4]Joint Institute for Nuclear Research, JINR Dubna, Russian Federation

E-mail: Andrei.Kazarov@cern.ch

Abstract. The ATLAS Trigger and Data Acquisition (TDAQ) is a large, distributed system composed of several thousands interconnected computers and tens of thousands software processes (applications). Applications produce a large amount of operational messages at the order of 10^4 messages per second, which need to be reliably stored and delivered to TDAQ operators in a quasi real-time manner, and also be available for post-mortem analysis by experts.

We have selected SPLUNK, a commercial solution by Splunk Inc, as an all-in-one solution for storing different types of operational data in an indexed database, and a web-based framework for searching and presenting the indexed data and for rapid development of user-oriented dashboards accessible in a web browser.

The paper describes capabilities of the Splunk framework, use cases, applications and web dashboards developed for facilitating the browsing and searching of TDAQ operational data by TDAQ operators and experts.

Trigger and Data Acquisition of the ATLAS experiment at LHC

ATLAS Experiment

A Toroidal LHC ApparatuS (ATLAS) [1] is a particle physics experiment at the Large Hadron Collider (LHC) at CERN. The LHC is producing proton-proton head-on collisions with center-of-mass energy equal to 13 TeV at 40 MHz collision rate. The ATLAS detector comprises more than 140 million electronic channels which deliver raw event data at the rate of order of TB/s.

Trigger and Data Acquisition system (TDAQ)

TDAQ is one of the core ATLAS systems [2] with the following key characteristics :

- Manages filtering and transfer of ATLAS experiment data from the detector to large-scale mass-storage, handles the flow of 1.5 MB events at rate up to 100 kHz
- A distributed computing system with more than 40000 applications running on a cluster of 2300 nodes
- Non-stop operation 24 hrs/day, 7 days/week during LHC Run 1 and Run 2
- Includes applications and frameworks for Configuration, Control and Monitoring the overall ATLAS data taking activity

One of the TDAQ applications is described in this paper.

Motivations for the use of SPLUNK for archiving and visualization

TDAQ applications produce a huge number of operational monitoring data on-line, which is necessary to gather, to archive, to process, to analyse and finally to present to the ATLAS operations crew and to experts to facilitate on-line supervision of the system and also for post-mortem analysis. This includes, in particular, a large amount of operational messages (at the order of O(10^4) messages per second), and other types of data like statistics of the busy fraction induced by ATLAS detectors.

SPLUNK, a commercial solution by Splunk Inc [3] was selected as an all-in-one solution for storing different types of operational data in an indexed database, and a web-based framework for searching, analysing and presenting the data. An important feature of Splunk is that it allows rapid development and easy maintenance of web applications, including user-oriented and task-oriented dashboards accessible in a web browser.

Splunk is developed as a system for archiving and processing of applications logs produced by processes running on large-scale clusters, which nicely can be extended to any type of textual operational data present in the TDAQ system.

SPLUNK workflow

The Splunk server (also called *indexer*) can receive data from files, TCP sockets or from the standard output of user scripts. It is capable to index any type of textual data it receives, and data are immediately available in search queries and in dashboards. To achieve the desired search performance, one can provide Splunk with some information about the structure of inserted data, e.g. fields which need to be indexed. TDAQ data are well-structured 'field=value' events, and for each type of events we developed a 'properties' configuration file, that gives Splunk an idea of which fields need indexing.

A typical event produced by the ERS (Error Reporting Service [4]) TDAQ application looks like:

```
t=1386776531, rn=224190, part=ATLAS, uname=crrc, msgID=rc::OngoingTransition, host=pc-tdq-onl
-77, app=RootController, sev=INFO, text="Transition INITIALIZE from IGUI is ongoing.", context="
PACKAGE_NAME: RunController. FILE_NAME: ../src/lib/RootController.cc. FUNCTION_NAME: virtual
void daq::rc::RootController::receive(const char*, const char*, const char*). LINE_NUMBER: 316.
DATE_TIME: 1386776531.", params="trans: INITIALIZE from IGUI. ", quals="RunController ", chained
="0", gh=1755720156
```

Which is indexed by Splunk with the help of this indexing configuration:

```
[ers]
TIME_PREFIX = ^t=
MAX_TIMESTAMP_LOOKAHEAD = 20
SHOULD_LINEMERGE = true
BREAK_ONLY_BEFORE = ^t=\d{10},\srn=\d+,\s
SEGMENTATION = ers
EXTRACT-fields = ,\stext="(?<text>.*)",\scontext="(?<context>.*)",\sparams="(?<params>.*)",\
squals="(?<quals>.*)",\schained=(?<chained>.+),\sgh=\d+$
```

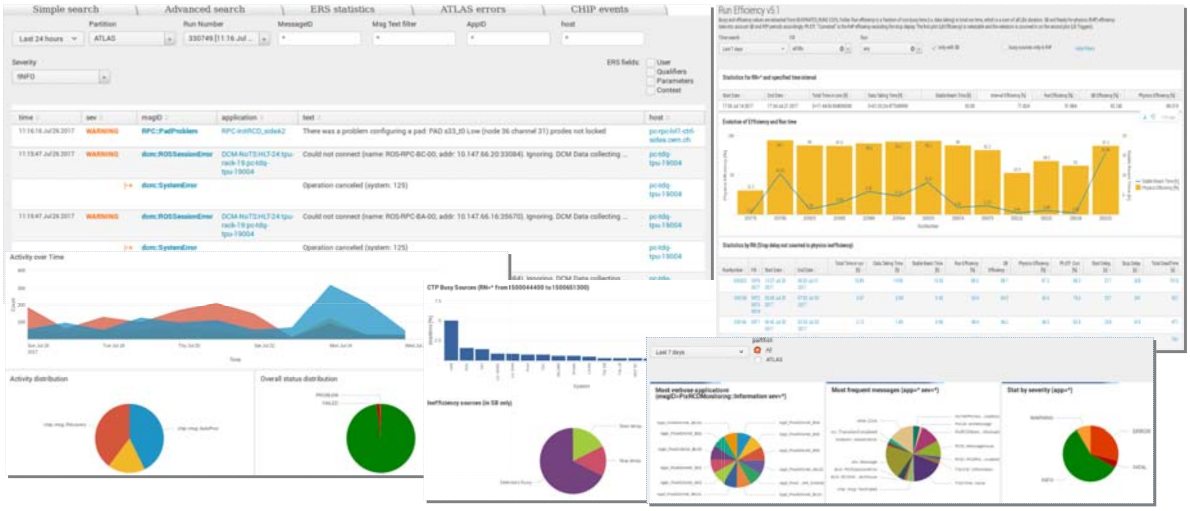
After the data are indexed, a process of getting results out of Splunk can be presented as a pipeline:

```
search(filter) | process(analyze, transform) | present(chart, dashboards)
```

where the (search | process | present) chain is literally a typical Splunk search string - a pipeline of commands, passing results to each other. A search is usually a selection of interesting fields by value. For processing the search results Splunk offers a great spectrum of functions: statistical, aggregation, transformation etc. Finally, selected and processed data are presented to the user in the form of tables, different forms of charts and plots which can be integrated into web pages as ready-to-use dashboards. The user is also allowed to work with the raw 'search' Splunk application, and to analyse data with a pipeline of Splunk commands. Below is an example search string from one of the TDAQ Splunk application demonstrating usage of Splunk search and processing capabilities:

```
search index=daqeff sourcetype=daq_eff Fill=* | dedup LumiBlock RunNumber | eval eDurRFP=
Duration*ReadyForPhysics*Eff | eval DurSB=Duration*StableBeams | eval eRTSB=Duration*StableBeams
*Eff | eval eRT=Duration*Eff | eval endT=_time+(Duration/1000) | eval SB1=case(StableBeams=1,
_time) | eval R4P1=case(ReadyForPhysics=1,_time) | eval inEff=(1-Eff)*Duration | chart eval(
round(sum(DurSB)/3600000,2)) as "Stable Beam Time [h]", eval(round((sum(eDurRFP)/sum(DurSB))
*100,1)) as "Physics Efficiency [%]" by RunNumber | sort RunNumber
```

Typically a Splunk application includes a number of dashboards which hide the complexity of data processing from the end users. Dashboards can be developed in a simple XML format, also they can be converted to the HTML format where the full power of JavaScript can be used to add more functionality if needed. A very useful feature for operational monitoring are real-time search forms and dashboards, where information is refreshed automatically as soon as fresh data get indexed.



time	sev	msgID	application	text	host
11:16:16 Jul 26 2017	WARNING	RPC::PadProblem	RPC-initRCD_sideA2	There was a problem configuring a pad: PAD s33_t0 Low (node 36 channel 31) prodes not locked	pc-rpc-lvl1-ctrl-sidea.cern.ch
11:15:47 Jul 26 2017	WARNING	dcm::ROSSessionError	DCM-NoTS:HLT-24:tpu-rack-19:pc-tdq-tpu-19004	Could not connect (name: ROS-RPC-BC-00, addr: 10.147.66.20:33084). Ignoring. DCM Data collecting ...	pc-tdq-tpu-19004
	⊢+	dcm::SystemError		Operation canceled (system: 125)	pc-tdq-tpu-19004
11:16:47 Jul 26 2017	WARNING	dcm::ROSSessionError	DCM-NoTS:HLT-24:tpu-rack-19:pc-tdq-tpu-19004	Could not connect (name: ROS-RPC-BA-00, addr: 10.147.66.16:35670). Ignoring. DCM Data collecting ...	pc-tdq-tpu-19004
	⊢+	dcm::SystemError		Operation canceled (system: 125)	pc-tdq-tpu-19004

Figure 1: Dashboards from TDAQ Splunk applications.

DAQ applications implemented in SPLUNK

A single Splunk server can host a number of independent applications, thus reducing the deployment and maintenance efforts. The TDAQ Splunk server hosts four applications, each handling specific type of data coming from different sources:

ERS web browser Provides access to millions of ERS messages produced by TDAQ applications in a web browser. It allows searching the messages based on run number, application name, host, severity, message text etc. Results are available in a table and can be exported. More advanced dashboards with statistics of messages (per application, severity and message type) are available for experts. ERS messages are collected from all running TDAQ applications and stored in files in an intermediate buffer on a shared filesystem before being indexed by Splunk.

Run efficiency dashboards Detailed information about ATLAS data-taking efficiency (fraction of dead-time induced by ATLAS detectors per lumi-block) is stored by the Central Trigger in an Oracle database. It is being indexed by Splunk, and a number of dashboards are available for experts, allowing to examine the efficiency evolution by run and to analyze sources of inefficiency by subsystem and by type.

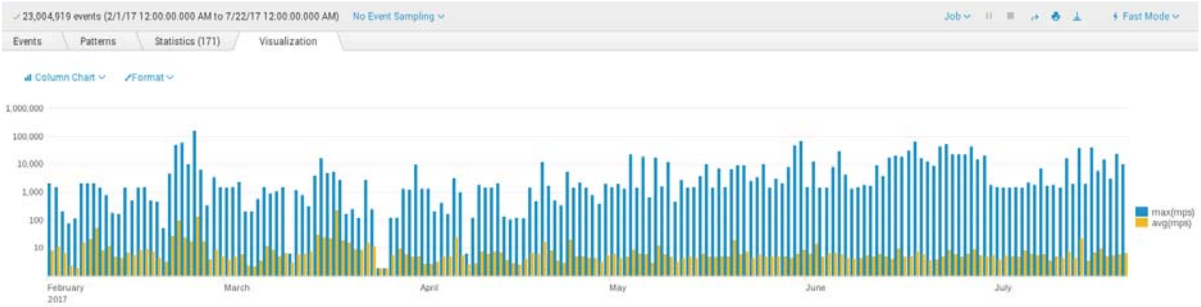
CHIP actions dashboard CHIP [5] is a central expert-system like application, aiming to automate different operational and recovery procedures. This Splunk application includes few dashboards which present the history and distribution of actions performed by CHIP.

Access Manager logs browser This is a classical Splunk application, where log files from distributed Access Manager [6] server instances are collected and indexed by Splunk, and a number of dashboards are provided with filtered information relevant for different use cases. This application is under development.

Screenshots of the dashboards from first three applications are presented on Figure 1.

Performance

A single Splunk server running on a virtual machine node (four cores, 7GB RAM) can handle the rates of events coming from TDAQ data sources as presented on Figure 2. In total more then 26M of messages were indexed, taking 16GB of the disk space.



✓ 23,004,919 events (2/1/17 12:00:00.000 AM to 7/22/17 12:00:00.000 AM)

Figure 2: Maximum and average number of messages indexed per second, for all data collected in course of 2017. This is a visualization of the results of a Splunk query.

Conclusions and outlook

Splunk is successfully used as an all-in-one solution framework for archiving and visualizing of the TDAQ operational data, providing easy integration, fast web applications development and low maintenance costs. An open-source solution, also adopted by CERN, like combination of Elastic Search and Kibana are considered for evaluation as a possible alternative.

References

[1] ATLAS Collaboration 2008 *Journal of Instrumentation, vol.* **3** S08003
[2] M Abolins et al 2016 *JINST 11* **06** P06008
[3] Splunk web page `www.splunk.com`
[4] S Kolos, A Kazarov and L Papaevgeniou 2015 *J. Phys.: Conf. Ser.* **608** 012004
[5] G Anders, G Avolio, G Lehmann Miotto and L Magnoni 2015 *J.Phys.Conf.Ser.* **608** 1, 012007
[6] M Valsan et al 2011 *J.Phys.Conf.Ser.* **331** 022042