.conf2015

Keep Your Eyes on The KPIs!

Enhancing Reliability with Splunk Alarming

Matthew Modestino

Design Specialist, Telus

splunk>

Disclaimer

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 the 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.

Agenda

- Introduction
- Monitoring key performance indicators (KPIs) with Splunk
- Creating Splunk alerts
- Creating Splunk alerting scripts to send SNMP traps
- Success stories

Hi My Name is….

Hello My Name Is…

Matthew Modestino

- Design Specialist, National Network Integrity, Telus
- 24x7 Tier 3 network and client experience assurance
- New technology introduction, subject matter expert
- Splunk Technical Champion, Certified Knowledge Manager
- n00bn0m0/n00badmin On Splunk IRC/Splunk Answers

TELUS

- Canada’s 2nd largest mobile carrier, 8.35 million subscribers
- Industry leading client retention through customer first culture
- Intense focus on “likelihood to recommend”

Likelihood to Recommend…

NEVER LET THE CLIENT BE THE FIRST TO TELL YOU THERE IS AN ISSUE!!

Key Performance Indicators

- What’s normal?
- What’s the trend?
- What’s the impact?
- Engineering/capacity measures

Gathering Intel…..

- Vendor equipment management systems
- CLI Commands/Health check script outputs/Logging
- Wire capture / Probes solutions
- Design docs/SME knowledge

Pros:

Amazing for bulk SNMP collection!

50k+ data sources in one place!

Aggregation of KPI, single pane of glass/Service alarming!

FREE!

Cons:

Severely outdated UI!

Non enterprise grade code, too much customization needed!

Lacks advanced analysis tools/visualizations,

Doesn’t support wide array of data types (without shoehorn)

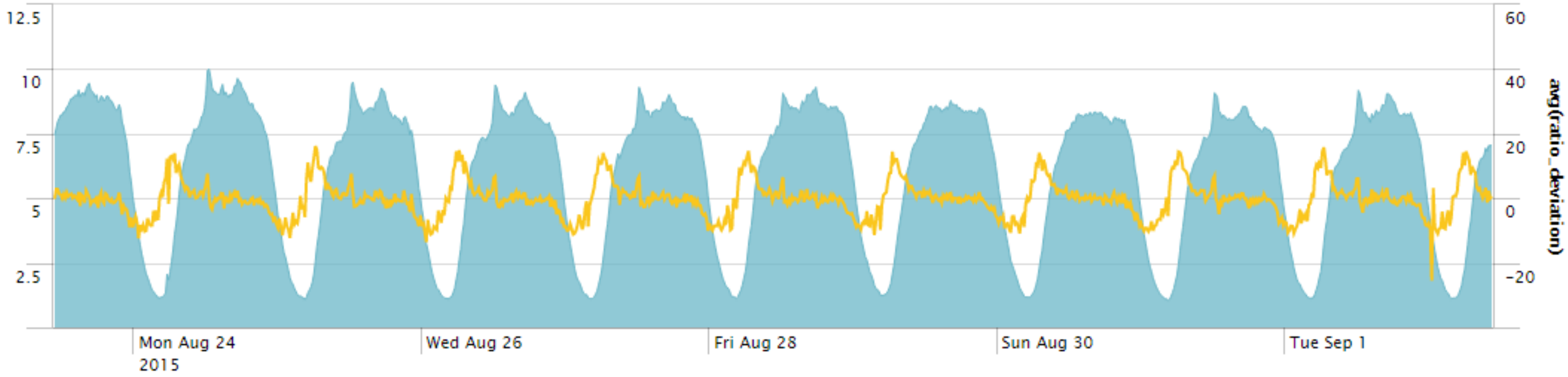
No product support

And then along came

splunk>®

Ingest/Identify/Trend Workflow

Ingest/Identify/Trend



Identify your critical KPIs…

Interface traffic Deviation, TPS thresholds, success rates, log events

Study these indicators and their meaning/criticality

Decide on alarming thresholds that need OPS engagement/Investigation

Create a Splunk Alert

Create Splunk Alerts

- http://docs.splunk.com/Documentation/Splunk/latest/Alert/Aboutalerts

- Create a search that isolates your alarm condition, then save as an alert.
- Use emails for the onboarding stage
- Collect SME knowledge and draft a "playbook"
- Once the alarm is tested and proven…

Create an Alert Script to Send SNMP Traps

SNMP to Other Systems

- http://docs.splunk.com/Documentation/Splunk/latest/alert/SendingSNMPtrapstoothersystems
- Stock Splunk example above utilizes perl and net-snmp to craft snmp traps to send to other systems
- The example provided in the alerting manual is a good way to get started with SNMP trapping from Splunk, however we quickly identified some need customization for our use….

Splunk Alerting Arguments

- Stock arguments only provided us with 3 items we had any interest in,
- chose to skip the step of passing args to our alert scripts to get the project moving….

```
$searchCount = $ARGV[0]; # $1 - Number of events returned
$searchTerms = $ARGV[1]; # $2 - Search terms
$searchQuery = $ARGV[2]; # $3 - Fully qualified query string
$searchName = $ARGV[3]; # $4 - Name of saved search
$searchReason = $ARGV[4]; # $5 - Reason saved search triggered
$searchURL = $ARGV[5]; # $6 - URL/Permalink of saved search
$searchTags = $ARGV[6]; # $7 - Always empty as of 4.1
$searchPath = $ARGV[7]; # $8 - Path to raw saved results in Splunk instance (advanced)
```

NET-SNMP HOMEWORK

- http://www.net-snmp.org/wiki/index.php/TUT:snmptrap

- In our proof of concept we simply used canned bash scripts that sent snmp traps using snmp v1
- We chose SNMP v1 based on some alert mapping options it allows when integrating to IBM Netcool

```
 [root@matt-vm01 labuser]# snmptrap -v1 -c public 192.168.100.1 "1.3.6.1.4.1.27389.99 192.168.200.1
6 1 1.3.6.1.4.1.27389.99.1.1 1.3.6.1.4.1.27389.99.1.1 s "PROBLEM" 1.3.6.1.4.1.27389.99.1.2 i "5"
1.3.6.1.4.1.27389.99.1.3 s “FIREWALL01" 1.3.6.1.4.1.27389.99.1.4 s “FIREWALL01 Dashboard"
1.3.6.1.4.1.27389.99.1.5 s "SPLUNK SAYS:ABNORMALLY LOW INTERNET TRAFFIC TREND"
1.3.6.1.4.1.27389.99.1.6 s "https://192.168.200.1/en-US/app/firewall01/firewall01"
1.3.6.1.4.1.27389.99.1.7 s "SPLUNK-KPIdeviation"
```

Example SNMPTRAP BREAKDOWN

- snmptrap -v1 -c public 192.168.100.1
- "1.3.6.1.4.1.27389.99 192.168.200.1 6 1 1.3.6.1.4.1.27389.99.1.1
- 1.3.6.1.4.1.27389.99.1.1 s "PROBLEM"
- 1.3.6.1.4.1.27389.99.1.2 i "5"
- 1.3.6.1.4.1.27389.99.1.3 s “FIREWALL01"
- 1.3.6.1.4.1.27389.99.1.4 s “FIREWALL01 Dashboard"
- 1.3.6.1.4.1.27389.99.1.5 s "SPLUNK SAYS: YOU GOT PROBLEMS!!! "
- 1.3.6.1.4.1.27389.99.1.6 s "https:// 192.168.200.1 :8000/en-US/app/firewall/FIREWALL01 "
- 1.3.6.1.4.1.27389.99.1.7 s "SPLUNK-KPIdeviation"

Clean up When You are Done…

- Generally it is a good practice to not only alarm, but to then clear those alarms when you are back to “normal”.
- To accomplish this we used the KVSTORE.
- THANKS MENNO VANDERLIST!!!
- http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/ConfigureKVstorelookups

Populate the KVSTORE

- In our search that triggered the SNMP script we also appended a output to a KVSTORE, which included a pre-defined key

```
|where attach_sr<=72.5
| eval _key= "sgsn02"
| table time _key host attach_sr
| outputlookup kvtest_lookup
```

API Call to Clear the KVSTORE

We then created a mirror search to our alert script which would watch the KVSTORE for an entry, then once found would check to see if the Normal condition was met.

```
curl -k -u alertuser:password -X DELETE \ https://192.168.200.1:8089/
servicesNS/nobody/system/storage/collections/data/alert_kvstore/sgsn02
```

http://www.georgestarcher.com/splunk-alert-scripts-automating-control/

“changing Splunk from a tool into a team member”

Create an Alert Script to Send SNMP Traps, Phase 2

Phase 2 Alarming…

- Phase 2 – Dynamic Alert Scripting using Alert Args
  - $searchName = $ARGV[3]; # $4 - Name of saved search
  - $searchURL = $ARGV[5]; # $6 - URL/Permalink of saved search
  - $searchPath = $ARGV[7]; # $8 - Path to raw saved results in Splunk instance (advanced)
- Enhance the alarms with search results/Values.
- Scott Haskell , ZENOSS Add-on - https://splunkbase.splunk.com/app/2766/
- We have yet to implement as we are having a lot of success with the phase 1 approach, but it is definitely in the pipeline

Splunk> WINS!

Splunk> Wins!

- Rich intel provided by the NOC and to engaged techs
- Reduced MTTR!!
- I can sleep at night!!
- Custom intelligent alarming created in house. ($$$)
- Grow Splunk awareness

.conf2015

Questions

splunk>

.conf2015

THANK YOU!!

splunk>