Splunk at Genesco

How we achieved a rapid ROI using Splunk to monitor application logs

Join the PonyPoll! Go to http://ponypoll.com/Genesco
Splunk at Genesco

How we achieved a rapid ROI using Splunk to monitor application logs

Jeremy Haggard | Manager Platform Systems & Certified Splunk Admin
Michael Nobles | Senior Sales Engineer & Splunker

2017 | Washington, DC
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.
Speaker Intro
Who are we and why are we here?

Jeremy Haggard
Manager Platform Systems
Genesco, Inc.
Nashville Splunk User Group Leader
Husband to my wife Misty and Dad to my daughter Allison.

Michael Nobles
Senior Sales Engineer
Splunk (based out of Atlanta)
Happily married to my wife Janelle for 26 years.
Four kids, two grown and married, two still at home.
You will learn.. 

…new exploration techniques for various areas within your machine data.
Todays Agenda

Forensics
Domain Admins

App Monitoring
Point of Sale

Splunk Apps
Free and Custom

Q & A
Join the Pony Poll, win some schwag!

ponypoll.com/Genesco
Who is Genesco?

We are an international, retail company based in Nashville TN
What does Splunk machinery look like at Genesco?
Data Flows and Splunk Architecture
High-level Environment Overview
Splunk Usage
High Level Summary

- 167,724,610 Events Per Day
- 5,031,738,300 Events Per Month
- 60,380,859,600 Events Per Year
- 83 Hosts
- 1,226 Sources
- 60 Source Types
Splunk Team @ Genesco

You don’t need a full time Splunk team to get a ROI
Genesco’s Journey

Forensics, POS (point of sale) and Useful Apps
The Problem:

- We had a legacy account enabled on our network.
  - It was used for an old application service years ago, but was never disabled.
  - Last activity time on account was < 2 weeks.
  - Active timestamp would update approx every 2 weeks.
  - No leads when looking at Palo Alto logging.

The question:

- What would break if we just disabled this old account?
- What services/applications were hardcoded to use it that we didn’t know?
Knowing WHERE to look was the key Splunk provided.

- **Research started**
  May 4, 2016
  Manual Process for 5 days.

- **Splunk Alerts Triggered – Event Analyzed**
  May 16, 2016 – May 23, 2016
  Real-Time searches prove value.
  Index= UserActivity "username"

- **Splunk Trial Installed**
  May 9, 2016
  Data Ingest Started on Domain Controllers

- **All Clear to disable the account**
  May 25, 2016

- **Last remnants removed**
  May 24, 2016
“For a moment, nothing happened. Then, after a second or so, nothing continued to happen.”

“The Hitchhiker’s Guide to the Galaxy” - Douglas Adams
APP MONITORING

POINT OF SALE
“Big things have small beginnings.”

T.E. Lawrence (Lawrence of Arabia) / Michael Fassbender (Prometheus)
We have many thousands of errors in the logs in dev. Someone needs to look at all of these. Inside the file “errors.tgz” is where I was just pulling out the word “ERROR” from the logs and ended up getting 63,356 lines worth of data. The errors themselves are in the log files and need immediate attention. There is no way to know what is working and what is not with this many errors.

Still growing, now at 133,247 lines of errors… I think Joe should be looking at this instead of scanner upgrades.

Still many errors out there getting generated... Logs attached.

I got this.
What the machine data looks like

2017-08-08 16:27:25,250 ERROR [ReplicationResequencingPublisher_6::0{549}.<1234] [FAILED_PERSISTENCE_LOG] Persistence Failed: dtv.data2.access.exception.PrimaryKeyViolationException: java.sql.SQLIntegrityConstraintViolationException: ORA-00001: unique constraint (DTV.PK_INV_INVCTL_TRANS_DETAIL) violated by -- > java.sql.SQLException: ORA-00001: unique constraint (DTV.PK_INV_INVCTL_TRANS_DETAIL) violated 2017-08-08 16:27:28,414 ERROR [ReplicationResequencingPublisher_6::0{549}.<1234] [dtv.data2.access.pm.PersistenceManager] Primary Key Violation while persisting object:

dtv.xst.dao.inv.impl.InventoryDocumentDAO@9df1254
Id: [98765432::SHIPPING::6::5555}
DaoState: [UPDATE] Id: 98765432
Values: documentId=5851452
documentTypeCode=SHIPPING
organizationId=6
retailLocationId=6205
createDate=2017-08-07 17:58:00.545
createUserId=0
updateDate=2017-08-08 16:32:54.139
updateUserId=989898
createDateTime=2017-08-07 00:00:00.0
documentSubtypeCode=FOUND
originatorName=DIVISION NAME
lastActivityDate=2017-08-08 12:32:54.139
recordCreationType=HOME_OFFICE

inventoryDocumentLineNumber=1
shipQuantity=0


dtv.xst.dao.inv.impl.InventoryDocumentLineItemDAO@5851452
Id: [989898::SHIPPING::1::6::5555}
DaoState: [UPDATE] Id: [989898::SHIPPING::1::104::6::5555]
Values: documentId=647852
documentTypeCode=SHIPPING
inventoryDocumentLineNumber=1
organizationId=6
retailLocationId=5555
createDate=2017-08-07 17:58:00.548
createUserId=0
updateDate=2017-08-08 16:32:54.139
updateUserId=222333
inventoryItemId=9879871
lineItemTypeCode=ITEM
statusCode=OPEN
unitCount=0
unitCost=21
expectedCount=1
postedCount=0
postedCost=0
recordCreationType=STORE

inventoryDocumentLineNumber=1
shipQuantity=0


dtv.xst.dao.inv.impl.InventoryTransactionDetailDAO@9999999c
Id: [6::5555::1502150400000::2::4184::1]
DaoState: [INSERT] Id: [6::5555::987978900000::2::4422::1]
Values: organizationId=6
retailLocationId=5555
businessDate=2017-08-08 00:00:00.0
workstationId=1
transactionSequence=6543
Where we started
<table>
<thead>
<tr>
<th>Error Code</th>
<th>Error Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Where we ended</td>
</tr>
<tr>
<td>0</td>
<td>Where we ended</td>
</tr>
<tr>
<td>0</td>
<td>Where we ended</td>
</tr>
<tr>
<td>0</td>
<td>Where we ended</td>
</tr>
<tr>
<td>0</td>
<td>Where we ended</td>
</tr>
<tr>
<td>0</td>
<td>Where we ended</td>
</tr>
<tr>
<td>0</td>
<td>Where we ended</td>
</tr>
<tr>
<td>0</td>
<td>Where we ended</td>
</tr>
<tr>
<td>0</td>
<td>Where we ended</td>
</tr>
</tbody>
</table>

Note: The table continues with similar entries.
1. Identify the specific error you want to find
   • look at raw logs, events or Splunk statistics tab.

2. Build the SPL for that error
   • Index=AWSPROD "ERROR" "primarykeyexception"

3. Save the result as a dashboard widget.

4. Repeat.
Build your SPL and each time you make a new widget add the error to a master SPL to help you drill down to quickly get through every error.

Example:

```plaintext
index=AWSPROD "ERROR"
- NOT "The server sent HTTP status code 404"
- NOT "Failed to save replication data to db"
- NOT "FailedPersistence"
- NOT "PrimaryKeyViolationException"
- NOT "{gen.tax.washington.id"
- NOT "${gen.pos.control.number.max.wait.time.limit}"
- NOT "[qtp243497350-396]"
- NOT "String length must be a multiple of four"
- NOT "(REPQUEUE.PK_RPL_REPLICATION_DATA) violated"
- Etc……
```

Tip!

Easily move through your events by adding exclusions.

Even if you are starting with millions of events.
Pinpointing Error Origination

“This always happens” – Every end user ever

TRUTHS:

- Sometimes we don’t get the whole truth.
- Emotions get in the way when going across teams/depts.
- With data in hand
  - Quickly gets you to the issue.
  - Allows you to focus on the problem and not the perception.
- It’s hard to argue FACTUAL DATA.
“The system never works.”

An example scenario
POS Server Data Captured
Straight from application log files.

3,536,428 Total POS Events in one day
Can you spot the problems?
POS Server Data Captured

The timeline tells a story and reduces time to resolve

5,493 Errors

Added additional search criteria
POS Server Data Captured
Drill down further to capture the minute and second in time this started.

“Factual data is actionable data.”
POS Server Data Captured
Easily pin-point the source of the errors

26%< 13%< 4%
POS Server Data Captured
And see who is impacted using a number of views

Example SPL:  `index=awsprod error| stats count by tag::host`
Splunkbase Apps = Time Saver
Secret sauce to a fast ROI

SplunkBase:
- Splunk App for AWS
- NMON Performance by Octamis
- Splunk App for Windows Infrastructure
- Website Monitoring
- Template for Citrix XenApp
- Template for Citrix XenDesktop 7
- Palo Alto
- Detailed License Monitoring and Alerting for Splunk

© 2017 SPLUNK INC.
1. Setup and maintain a “sandbox”/Splunk Development area (obtain your own free, 50 GB/day Personal Developer license)

2. Feel free to run Splunk on your own machine to quickly explore new data and new Apps from the Splunkbase app "store"

3. Sign up for Splunk “Answers” and become part of the community

4. Google is your friend

5. Run Splunk (free version) at home to get even more value and more comfort

Tip! Be sure to research best practices
We currently use 10 custom apps to monitor our POS environment.

- These custom apps mostly run scripts on our Linux environment to pull specific data.
  - count of files, file permissions, md5sum, etc...

- **App/bin directory**
  - sample_script.sh

- **App/local directory**
  - Inputs.conf
    - [script://opt/splunkforwarder/etc/apps/sample_scripts/bin/sample_script.sh]
    - interval = 900
    - [monitor://opt/sample/logs/]
    - sourcetype = sample_script

Custom Apps
Easier than you think to get your data.
Summary

- Forensics
- Domain Admins

- App Monitoring
- Point of Sale

- Splunk Apps
- Free and Custom

- Q & A
Q&A

Jeremy Haggard | Genesco
Mike Nobles | Splunk
Explore

Explore your data without fear of the great unknown!
Thank You

Don't forget to rate this session in the .conf2017 mobile app

Jeremy@SplunkNashville.com