WEB APPLICATION MONITORING AND ANALYTICS WITH SPLUNK

INFORMATION TECHNOLOGY
UNIVERSITY OF WASHINGTON
AGENDA

- About Us
- What is Splunk?
- Splunk at the University of Washington
- Supporting an existing service
- Providing data to UX with client-side instrumentation
- Get Splunk for your department
ACADEMIC AND COLLABORATIVE APPLICATIONS

A division within UW-IT focused on building student facing Web applications

Must develop new applications while maintaining legacy applications with limited resources

Facts and figures

Small team of 6 engineers
Maintain ~15 applications
Support over 140,000 users across 3 campuses
Support 9 groups on campus running their own Splunk instances via our license master
WHAT WE MAINTAIN
MY BACKGROUND AND ROLE

> Stephen De Vight
> With the UW since 2006
> Current Role: Senior Computer Specialist, 2011
> Mission: To support teaching and learning on campus through the development of interactive Web and mobile applications
WHAT IS SPLUNK?
SPLUNK ENTERPRISE AT UW - 2012

aca-log

Universal Forwarders
SPLUNK ENTERPRISE AT UW - 2014

Universal Forwarders

‘External’ Splunk instances

splunk-search01

splunk-index01

splunk-index02

splunk-license
SUPPORTING AN EXISTING SERVICE

> Homegrown suite of academic applications
> Currently consists of 8 distinct tools
> Released in 1999
SUPPORTING AN EXISTING SERVICE

OUR NEEDS

> **Situation:** Legacy database logging system reached end of life, was not scaling well, and was too costly to directly replace

> **Struggling with:** Finding a solution that is both easy to build and maintain as well as being able to scale to our needs

> **Wanted:** An easy to use, UI-driven, application to search our log data

> **Enter Splunk:** Splunk Enterprise allowed us to build a custom searching app as well as a dashboard for monitoring service status
SUPPORTING AN EXISTING SERVICE

CATALYST LOG SEARCH

> Splunk application with advanced XML view
SUPPORTING AN EXISTING SERVICE

CATALYST LOG SEARCH

> Splunk application with advanced XML view
> Search form negates the need for users to learn Splunk search language or understand our log formatting and structure
SUPPORTING AN EXISTING SERVICE

CATALYST LOG SEARCH

> Splunk application with advanced XML view
> Search form negates the need for users to learn Splunk search language or understand our log formatting and structure
> Support can analyze user activity to provide insight into incident reports
SUPPORTING AN EXISTING SERVICE

CATALYST DASHBOARD

> Gauge current level of activity at a glance
> Examine last day of activity for anomalous usage
> Targets slowest loading URLs for performance improvement
DATA DRIVEN USER EXPERIENCE

Mobile Web version of our student portal

Focused on providing timely, actionable information to our students

Based on a student's situation and the time of the quarter we dynamically display, hide, move, and reorder content
DATA DRIVEN USER EXPERIENCE

OUR NEEDS

- **Situation:** UX needs a way to validate their assumptions around what content is relevant to a student at various points in the quarter.

- **Struggling with:** Correlating user activity with institutional data (e.g. class standing, campus, etc.).

- **Wanted:** A self-driven means for UX and business analysts to analyze log data.

- **Enter Splunk:** Splunk, along with our client-side logging solution, allows us to correlate user activity with certain institutional attributes we log.
DATA DRIVEN USER EXPERIENCE

CLIENT-SIDE LOGGING

> Google Analytics did not get us everything we needed
> Using log4javascript to collate events and POST to a REST interface
> Events are bundled to reduce network overhead
> Events are written to file by REST server

http://www.log4javascript.org/
DATA DRIVEN USER EXPERIENCE

WORKING WITH CLIENT LOGS

> Link Log
  > Link location
  > Target URL
  > Action (view, click)

> Card Log
  > Card location URL
  > Card name
  > Card position
  > Action (load, view, expand, collapse)

INFO 21 22:25:31
{
  "level": "INFO",
  "url": "https://my.uw.edu/mobile/landing/",
  "timestamp": 1421907930962,
  "logger": "link",
  "session_key": "xc63940325jlo3dsdfcgg3126b",
  "message": {
    "href": "http://gmail.uw.edu/",
    "action": "click"
  }
}
DATA DRIVEN USER EXPERIENCE

index=myuw_production
sourcetype=myuw_link_log
action=click
|stats count by target_url
DATA DRIVEN USER EXPERIENCE

SERVER-SIDE SESSION LOG

> Session Log
> Graduate or undergraduate
> Class standing
> Campus

INFO 21 22:21:20
{
  "is_grad": false,
  "netid": "javerage",
  "is_ugrad": true,
  "class_level": "FRESHMAN",
  "session_key": "xc63940325j1o3dsdfcgtt3126b",
  "campus": "seattle"
}
[session]
DATA DRIVEN USER EXPERIENCE

EVENTTYPES AND TRANSACTIONS

> Build an eventtype that contains both link and session logs

```
index=myuw_production
(sourcetype=myuw_link_log
OR sourcetype=myuw_session_log)
```
DATA DRIVEN USER EXPERIENCE

SESSION ACTIVITY WITH TRANSACTIONS

> Create a transaction based on session_key
> Find transactions that contain a link click to ‘*dars.asp’
> Get count of other URL targets clicked within that transaction

- Create a transaction based on session_key
- Find transactions that contain a link click to ‘*dars.asp’
- Get count of other URL targets clicked within that transaction

```
index=myuw_production
eventtype=link_event
|transaction_fields=session_key
maxspan=8h
|search target_url=*dars.asp
AND action=click
|stats count by target_url
```
DATA DRIVEN USER EXPERIENCE

COMBINING LOGS WITH TRANSACTIONS

> Create a transaction based on session_key
> Find link events that have a click action
> Using the session log, determine how many link clicks were made by each class level

```
index=muyw_production eventtype=link_event
|transaction_fields=session_key maxspan=8h
|search action=click
|stats count by class_level
```
TOP TAKEAWAYS

> Building a search form makes Splunk simple to use
> Determine your analysis needs before creating your logging scheme
> Client side logging can provide valuable insight into user behavior
> Transactions make combining logs easy
SPLUNK FOR YOUR DEPARTMENT

- Splunk is sold in terms of data indexed per day
- Discounted pricing available through Internet2
- Contact tomlewis@uw.edu for details

<table>
<thead>
<tr>
<th>Tier (GB)</th>
<th>Fees for Software and Support (total amount, payable over three years in annual installments)</th>
<th>Example Annual Payment</th>
<th>$/GB/yr</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>$44,577</td>
<td>$14,859/yr</td>
<td>743</td>
</tr>
<tr>
<td>50</td>
<td>$70,581</td>
<td>$23,527/yr</td>
<td>471</td>
</tr>
<tr>
<td>100</td>
<td>$111,447</td>
<td>$37,149/yr</td>
<td>371</td>
</tr>
<tr>
<td>200</td>
<td>$208,032</td>
<td>$69,344/yr</td>
<td>347</td>
</tr>
<tr>
<td>500</td>
<td>$482,937</td>
<td>$160,979/yr</td>
<td>322</td>
</tr>
<tr>
<td>1,000</td>
<td>$891,573</td>
<td>$297,192/yr</td>
<td>290</td>
</tr>
</tbody>
</table>
QUESTIONS?