Multi-Tenancy: Achieving Security, Collaboration, And Operational Efficiency

Dave Safian  |  Sr. Solutions Engineer
Ben August  |  Sr. Solutions Engineer

September 26, 2017  |  Washington, DC
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.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.
About The Presenters

- **Ben August**
  - Sr. Solutions Engineer, ITS Middleware Services
  - Higher Ed 10 years, UNC for 4 years
  - Splunk Certified Administrator

- **Dave Safian**
  - Sr. Solutions Engineer, ITS Middleware Services
  - Higher Ed 20 years, at UNC for 5 years
  - Splunk Certified Architect II
The University Of North Carolina At Chapel Hill

- Nation’s first public university
- 19k Undergraduate students
- 11k Grad/professional students
- 11k Faculty/staff
- $2.4B Annual budget
Carolina ITS By The Numbers

- 28,000+ Visits to walk-in Help Desk each year
- 68,000+ Operator assisted calls annually
- 22,000+ Software titles distributed annually
- 11+ Million inbound/outbound email messages per day
- 87,600 Active user accounts
- 50,000+ Computers provisioned and supported
- 50k Wired devices connect to network daily
- 60k Wireless devices connect to network daily
- 3923 Courses in LMS taught by 2,276 instructors
Campus Technology Challenges

- Open nature of higher education
  - Students using multiple personal devices on-campus
  - Interact with multiple systems throughout the day (web, LMS, student systems, email)
  - Students expect 24x7 access
  - Students active in social media when services are less than stellar

- Centralized and decentralized IT
  - 90+ departments who manage their own services
  - Some run their own servers, some run services hosted in ITS
  - All have similar reporting needs
Operational Challenges Within ITS
Supporting Mission-Critical Services

- Reactive to Issues (Not Proactive)
- Ad-Hoc Search Methods
- Hard to determine what data is relevant
- Lack of Holistic View of systems
- Finger Pointing / Lack of Factual Data
- Slow to resolve problems
- Complex Architecture
Data in many different systems managed as silos by different teams

Problems often present themselves across multiple tiers / nodes

All of these systems produce data widely varying different formats
Reporting Objectives
Achieving Operational Efficiency, Security, and Collaboration

We need to build a reporting platform where we can collect and analyze all of our data all in one place.

- Get data out of silos and into a space where multiple teams can access it
- Enable team to work through problems using a common “language”
- Trace transactions through the entire system stack
- Restrict data to prevent authorized access / snooping
- Follow a user as they move through multiple systems and across campus
- Detect malicious activity and compromised accounts
- Make machine data about services available to less technical folks
- Provide tools to front-line support staff to offload work from tier 3
- Provide campus IT departments the same reporting capability
The Solution: Splunk

1. Build a Robust Architecture (High Availability / Disaster Recovery
2. Get Data out of Silos
3. Support Multi-tenancy for IT operations many departments and colleges
4. Grow Splunk Expertise across organization through collaboration
5. Publish dashboards tools that benefit the entire organization
Step 1: Robust Architecture

- Load Balancer
- Search Head Cluster
- Indexing Cluster
- Manning Data Center
- Franklin Data Center
Step 2: Get The Data In
From all mission critical systems and infrastructure

▶ Firewall Logs (130GB/day)
▶ Active Directory, Exchange (180+GB/day)
▶ PeopleSoft (10k+ unique log files/week)
▶ WordPress, Sakai LMS, campus web servers
▶ LDAP, Kerberos, Single Sign-On
▶ Switches, DHCP, F5

* Unix

DB

WIN

VM
Step 3: Tackling Multi-Tenancy

How to organize data and access in Splunk?

- Provide means to restrict access to specific data sources
- Permit multiple teams access to specific data sets
- Use established infrastructure to manage roles and memberships
Supporting Data isolation
The role, index, and app connection

Role: ITS-Middleware
App: ITS Middleware
Index = middleware

Role: ITS-Networking
App: ITS Networking
Index = network

Role: SPH
App: School of Public Health
Index = sph
We own the service, not the data

Departments own:
- The data in their index
- The objects in their application
- The membership of their roles

We just proxy sharing requests and manage access

Disclaimer: ISO gets access to all your data!
Access Control Delegation

Existing Infrastructure Saves Time

▶ Splunk Roles tied to LDAP groups
  • Authorization and Role membership
▶ LDAP groups tied to Group Management System
  • Grouper used for managing group membership
  • Groups fed from HR departmental data where possible
  • AD Admin Groups
  • Otherwise delegated to a manager
▶ Single Sign-On (Shibboleth) for password management
▶ Ansible Tower/ Git for automation, configuration management, versioning
▶ We have 660+ users and 100+ roles!
Step 4: Building Expertise Through Collaboration

Splunk Ninjas in Every Cubicle

- Splunk Community
  - How-to’s on configuring forwarders
  - Best Practices
  - Users’ Contributions
- On-site Splunk Training
- Informal Training Sessions
- Splunk User Mailing list
- Twitter: @UNCSplunk
- Internet 2/ Splunk Free Training
Step 5: Building Enterprise-Class Reports

The Move to Institutional Reporting

- Start treating dashboards like enterprise tools
- One central location
- Controlled rollout of changes
- Validation of permissions
- Version Control
The Splunk Shared Tools App

- Houses all dashboards used by multiple teams
- The app is globally accessible, dashboards are not
- Dynamic menus
- Super-users Group manages change process
What UNC Does With Splunk

Achieving security, operational efficiency, and reporting

- Troubleshooting Tools for Support Staff
  - Account lockouts, Peoplesoft Troubleshooting
- Cross-department reporting and alerting on core University Systems
  - Campus Web (Wordpress), Financials/Student (Peoplesoft), LMS (Sakai)
- Self-Service reporting to Campus IT Departments for central services
  - Patch Management, Firewall Troubleshooting, Vulnerability Scanning
- Compromised account detection and alerting
- Malicious activity detection and alerting
Live Demo
Peoplesoft Troubleshooting
## Active Directory Lockouts

### Active Directory Lockout Troubleshooting

**Onyen**

<table>
<thead>
<tr>
<th>d*</th>
<th>Today</th>
</tr>
</thead>
</table>

**Active Directory Login Failures**

<table>
<thead>
<tr>
<th>Account_Name</th>
<th>AD Server</th>
<th>Server on Which Failed Authentication Occurred</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>skjeff</td>
<td>addc4</td>
<td>webdot0p</td>
<td>12/01/2016 04:10:43 PM</td>
</tr>
</tbody>
</table>

**Exchange Login Failures**

<table>
<thead>
<tr>
<th>Time</th>
<th>Account_Name</th>
<th>Server on Which Failed Authentication Occurred</th>
<th>Server Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/01/2016 12:56:35 PM</td>
<td>arbones</td>
<td>ITS-MSXHT6F</td>
<td>Exchange SMTP</td>
</tr>
<tr>
<td>12/01/2016 12:56:12 AM</td>
<td>kimmiche</td>
<td>ITS-MSXCA1</td>
<td>Exchange Client Access</td>
</tr>
</tbody>
</table>

**Direct Computer Login Failures**

<table>
<thead>
<tr>
<th>Time</th>
<th>Account_Name</th>
<th>Server on Which Failed Authentication Occurred</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/01/2016 04:12:20 PM</td>
<td>jvmarcus</td>
<td>dhcp191069.</td>
</tr>
</tbody>
</table>
Key Performance Indicators

- Average Response time: 0.134 s
- Successful Requests: 100%
- Requests per minute: 711

Logins per 5 minutes (by host over time range)

Concurrent Users

Request Distribution (web servers)
## Firewall Troubleshooting

<table>
<thead>
<tr>
<th>Source IP Address</th>
<th>Destination IP Address</th>
<th>Destination Port</th>
<th>Firewall Action</th>
<th>Perform DNS Lookup</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.17.35.196</td>
<td></td>
<td></td>
<td>All</td>
<td>No</td>
</tr>
</tbody>
</table>

### Time Range
- **Last 60 minutes**

### Source IP Address and Destination IP Address
Enter an IP address to search on. Leave empty to perform a wildcard (*) search of all IP addresses. Other wildcard values work as such as 192.19.250.* OR 192.19.250/24.

### Destination Port
Enter a destination port to search on. Leave empty to perform a wildcard (*) search on all ports.

### Firewall Action
Filter results by firewall action. Show ALL traffic, Allowed, Blocked, or Unknown traffic actions.

### Perform DNS Lookup
Attempt to translate IP addresses to hostnames. Doing so can substantially slow down search results.

### Time Range
Select time range to search over.

### Firewall Search Results

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Action</th>
<th>Firewall Address</th>
<th>vsys</th>
<th>Firewall Policy</th>
<th>Src Address</th>
<th>Src Zone</th>
<th>dest_ip_subnet</th>
<th>dest_zone</th>
<th>dest_port</th>
<th>Protocol</th>
<th>Pkts In</th>
<th>Pkts Out</th>
<th>Session End</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017/08/16 10:13:57</td>
<td>allowed</td>
<td>172.22.134.42</td>
<td>vsys6</td>
<td>ITSOSDMZP-0041</td>
<td>172.17.35.196</td>
<td>untrust</td>
<td>172.27.47.52</td>
<td>ITS-OS-DMZ-prod</td>
<td>tcp</td>
<td>8000</td>
<td>5</td>
<td>6</td>
<td>tcp-rst-from-client</td>
</tr>
<tr>
<td>2017/08/16 10:09:24</td>
<td>allowed</td>
<td>172.22.134.42</td>
<td>vsys6</td>
<td>MIDDLEWARE-0034</td>
<td>172.17.35.196</td>
<td>untrust</td>
<td>172.27.206.3</td>
<td>FS-DC-NoSNAT</td>
<td>tcp</td>
<td>443</td>
<td>10</td>
<td>9</td>
<td>tcp-fn</td>
</tr>
<tr>
<td>2017/08/16 10:09:24</td>
<td>allowed</td>
<td>172.22.134.42</td>
<td>vsys6</td>
<td>MIDDLEWARE-0034</td>
<td>172.17.35.196</td>
<td>untrust</td>
<td>172.27.206.3</td>
<td>FS-DC-NoSNAT</td>
<td>tcp</td>
<td>443</td>
<td>9</td>
<td>9</td>
<td>tcp-fn</td>
</tr>
<tr>
<td>2017/08/16 10:07:24</td>
<td>allowed</td>
<td>172.22.134.42</td>
<td>vsys6</td>
<td>MIDDLEWARE-0034</td>
<td>172.17.35.196</td>
<td>untrust</td>
<td>172.27.206.3</td>
<td>FS-DC-NoSNAT</td>
<td>tcp</td>
<td>443</td>
<td>10</td>
<td>9</td>
<td>tcp-fn</td>
</tr>
<tr>
<td>2017/08/16 10:07:24</td>
<td>allowed</td>
<td>172.22.134.42</td>
<td>vsys6</td>
<td>MIDDLEWARE-0034</td>
<td>172.17.35.196</td>
<td>untrust</td>
<td>172.27.206.3</td>
<td>FS-DC-NoSNAT</td>
<td>tcp</td>
<td>443</td>
<td>9</td>
<td>9</td>
<td>tcp-fn</td>
</tr>
<tr>
<td>2017/08/16 10:06:58</td>
<td>allowed</td>
<td>172.22.134.42</td>
<td>vsys6</td>
<td>MIDDLEWARE-0034</td>
<td>172.17.35.196</td>
<td>untrust</td>
<td>172.27.206.3</td>
<td>FS-DC-NoSNAT</td>
<td>tcp</td>
<td>443</td>
<td>10</td>
<td>9</td>
<td>tcp-fn</td>
</tr>
<tr>
<td>2017/08/16 10:09:15</td>
<td>allowed</td>
<td>172.22.134.42</td>
<td>vsys6</td>
<td>MIDDLEWARE-0034</td>
<td>172.17.35.196</td>
<td>untrust</td>
<td>172.27.206.3</td>
<td>FS-DC-NoSNAT</td>
<td>tcp</td>
<td>443</td>
<td>10</td>
<td>9</td>
<td>tcp-fn</td>
</tr>
<tr>
<td>2017/08/16 09:57:59</td>
<td>allowed</td>
<td>172.22.134.42</td>
<td>vsys6</td>
<td>ERP-1449</td>
<td>172.17.35.196</td>
<td>untrust</td>
<td>152.19.220.16</td>
<td>ERP-DMZ</td>
<td>tcp</td>
<td>443</td>
<td>9</td>
<td>10</td>
<td>tcp-rst-from-client</td>
</tr>
<tr>
<td>2017/08/16 09:57:14</td>
<td>allowed</td>
<td>172.22.134.42</td>
<td>vsys6</td>
<td>ERP-1449</td>
<td>172.17.35.196</td>
<td>untrust</td>
<td>152.19.220.16</td>
<td>ERP-DMZ</td>
<td>tcp</td>
<td>443</td>
<td>11</td>
<td>12</td>
<td>tcp-fn</td>
</tr>
</tbody>
</table>
Vulnerability Detection
Benefits To UNC

- All logs, for all systems across campus
- Visibility across the entire enterprise
- Data becomes accessible and relevant to non-technical
- Better security
- Increased efficiency
- Proactive Monitoring and Alerting
- Common tool/language used by the organization
Thank You

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