

splunk> .conf2017

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.

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

Supporting Mission-Critical Services

-

IT Complexity In Core Business Services

Firewall

Routers, Switches, and Load Balancers

Web and Application Servers

Servers and OS

Authentication / Directory Servers

Storage

Databases

Virtualization

- ▶ 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

Achieving Operational Efficiency, Security, and Collaboration

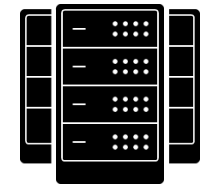
We need to build a reporting platform where we can collect and analyze all of our data all in one place.

- ▶ 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 unauthorized 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

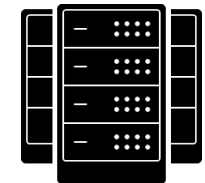
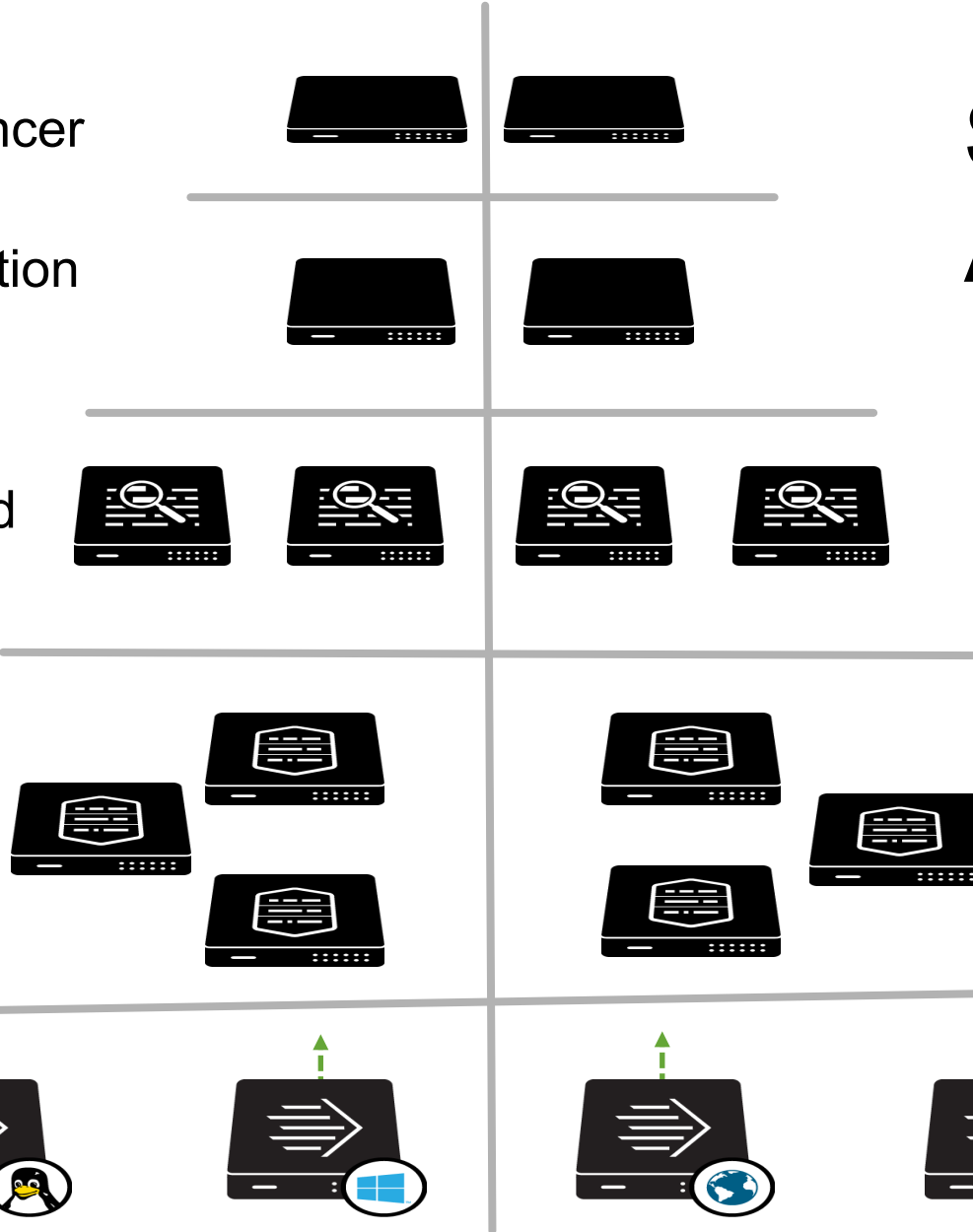


Manning
Data
Center

Load Balancer
Web & Authentication

Search Head
Cluster

Indexing
Cluster



Franklin
Data Center



- 
- WIN**

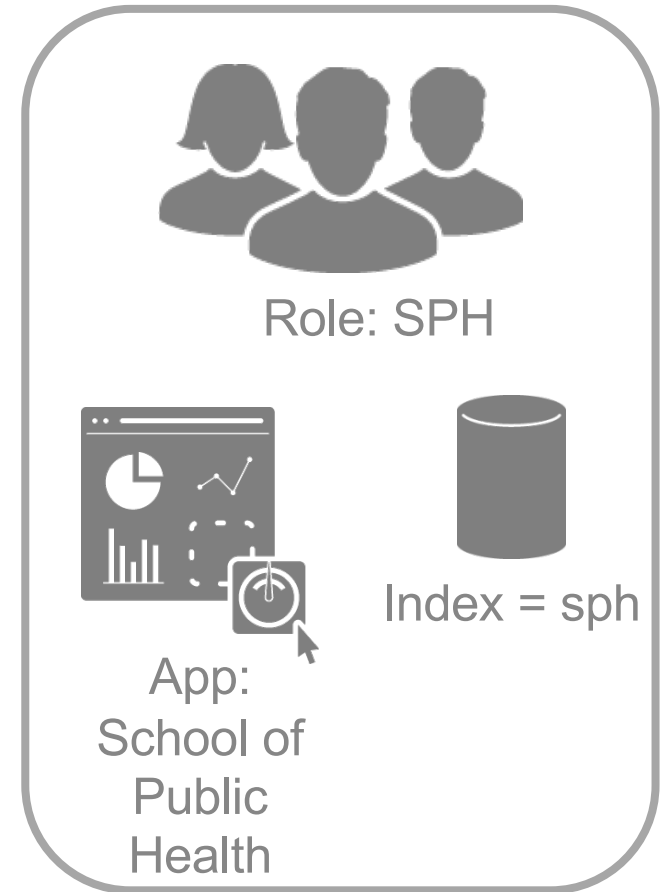
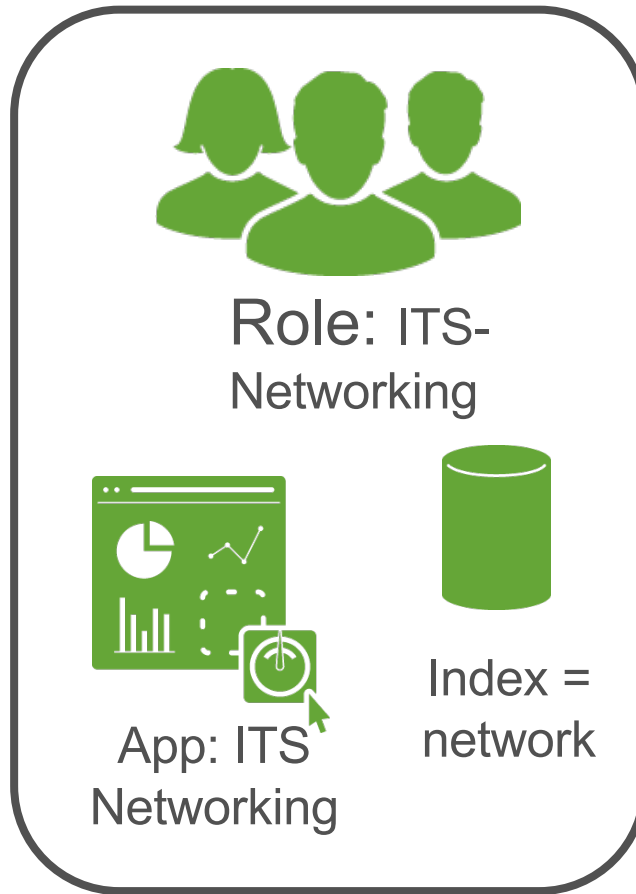
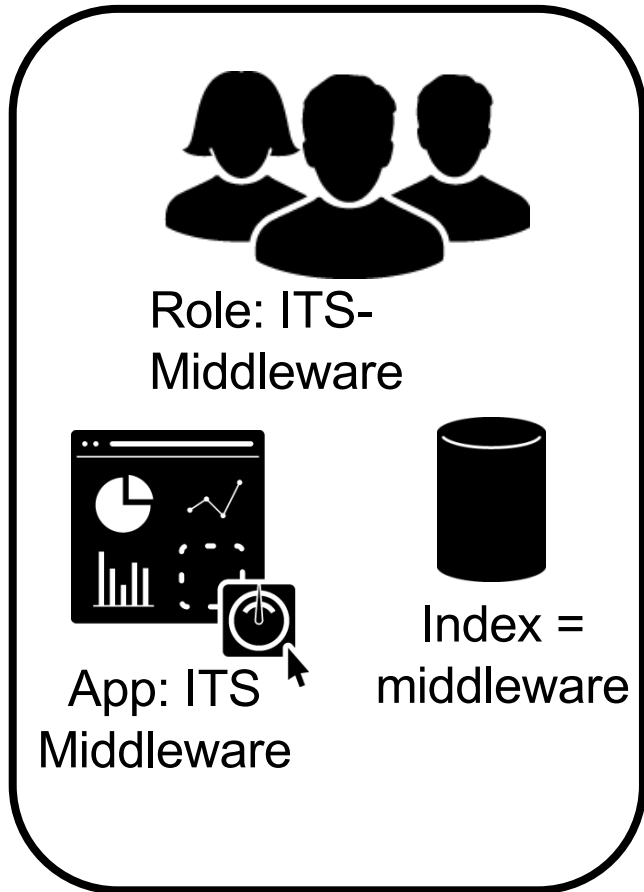
VM

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



Supporting Data Sharing

Delegated Ownership Model

- ▶ 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!

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.189
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D18SLBFF3ADFF9 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=FI-SW-03" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.189
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.189
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D18SLBFF3ADFF9 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=FI-SW-03" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.189
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.189
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D18SLBFF3ADFF9 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=FI-SW-03" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.189

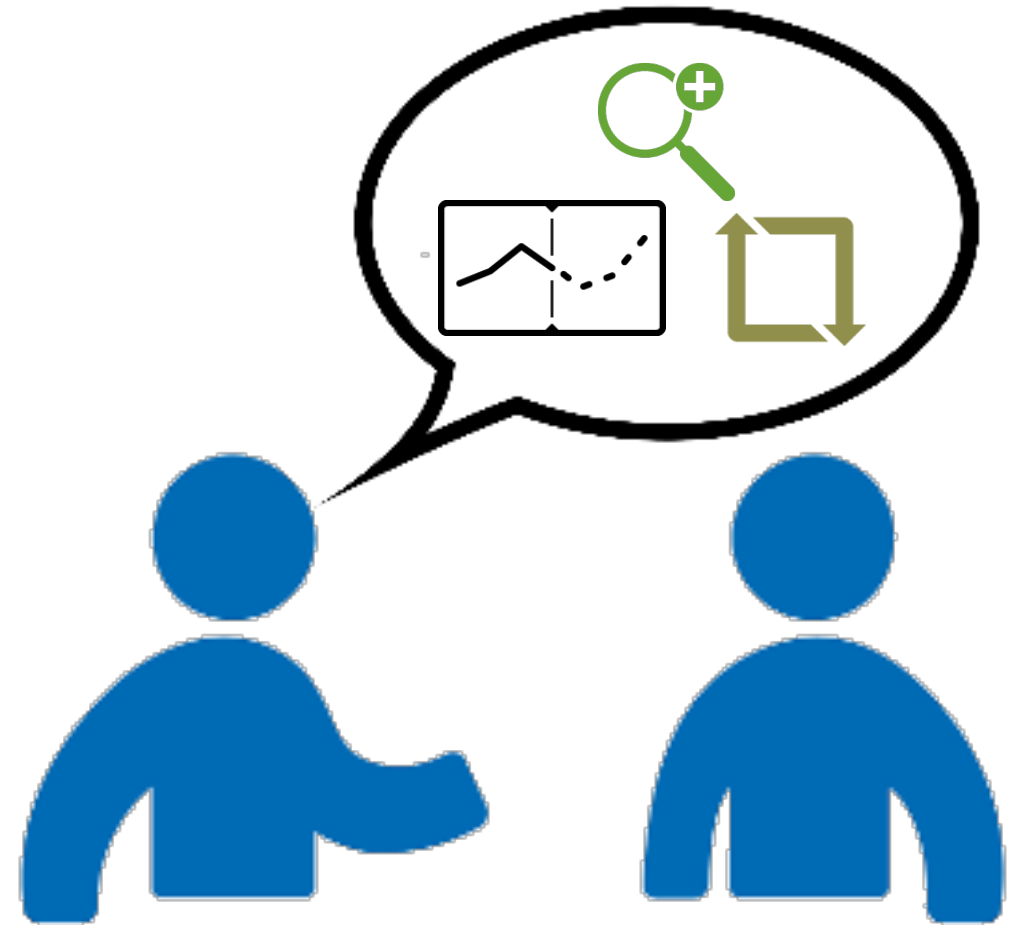
Existing Infrastructure Saves Time

- 

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: @UNCSSplunk
- ▶ Internet 2/ Splunk Free Training



The Move to Institutional Reporting

-

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



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03" "Opera/9.80 (Macintosh; Intel Mac OS X 10_11_0; rv:52.0) Gecko/20100101 Firefox/52.0"

128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D3SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:52.0) Gecko/20100101 Firefox/52.0"

317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D18SLBFF3ADFF9 HTTP 1.1" 200 3855 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-14&product_id=K9-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:52.0) Gecko/20100101 Firefox/52.0"

10 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D18SLBFF3ADFF9 HTTP 1.1" 200 3855 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-14&product_id=K9-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:52.0) Gecko/20100101 Firefox/52.0"

10 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D18SLBFF3ADFF9 HTTP 1.1" 200 3855 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-14&product_id=K9-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:52.0) Gecko/20100101 Firefox/52.0"

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

130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03"
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
317 27.160.0.0 - - [07/Jun 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"
itemId=EST-16&product_id=RP-LI-02" 468 125.17 14.189 "GET /category.screen?category_id=FLOWERS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"
ofaction=purchase&itemId=EST-26&product_id=RP-LI-02" 468 125.17 14.189 "GET /category.screen?category_id=FLOWERS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"
ofaction=purchase&itemId=EST-26&product_id=RP-LI-02" 468 125.17 14.189 "GET /category.screen?category_id=FLOWERS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=F1-SW-03"

Live Demo

Peoplesoft Troubleshooting

Splunk Infrastructure ▾ Active Directory and Messaging ▾ Security and Firewall ▾ Enterprise Applications ▾ Networking ▾ ITSApps ▾ Middleware ▾ Splunk Shared Tools

ConnectCarolina Troubleshooting

Onyen: dsafian IP Address: 172.17.35.196 PID: 7 7 Last 24 hours Submit Hide Filters

Landing Page (connectcarolina.unc.edu) Access Data

Date/Time ▾	IP Address ▾	Domain ▾	Path ▾	HTTP Status ▾	HTTP Referer ▾	User Agent ▾
08/16/2017 09:56:11.536	172.17.35.196	connectcarolina.unc.edu	/	200		Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.90 Safari/537.36

Shibboleth Audit Data

Date/Time ▾	Onyen ▾	Client IP ▾	Service Provider ▾	Identity Provider (IdP) ▾	IdP Host ▾
08/16/2017 09:56:21	dsafian	172.17.35.196	https://hcrpt.cc.unc.edu/shibboleth	https://sso.unc.edu/idp	ssoapp0p
08/16/2017 09:56:20	dsafian	172.17.35.196	https://fsrpt.cc.unc.edu/shibboleth	https://sso.unc.edu/idp	ssoapp0p
08/16/2017 09:56:20	dsafian	172.17.35.196	https://csrpt.cc.unc.edu/shibboleth	https://sso.unc.edu/idp	ssoapp0p
08/16/2017 09:56:20	dsafian	172.17.35.196	https://hc.cc.unc.edu/shibboleth	https://sso.unc.edu/idp	ssoapp0p

ConnectCarolina Grey Heller Access Data

Date/Time ▾	Content Provider ▾	Onyen ▾	IP ▾	menu ^	component ▾	page ▾	keys ▾
2017-08-16 09:56:41	hcprd	dsafian	172.17.35.196	ROLE_EMPLOYEE	PY_IC_PAY_INQ		
2017-08-16 09:56:43	paprd	dsafian	172.17.35.196	ROLE_EMPLOYEE	PY_IC_PAY_INQ		
2017-08-16 09:56:44	hcprd	dsafian	172.17.35.196	ROLE_EMPLOYEE	PY_IC_PAY_INQ	PY_IC_PL_LIST	
2017-08-16 09:56:59	hcprd	dsafian	172.17.35.196	ROLE_EMPLOYEE	PY_IC_W4		
2017-08-16 09:57:00	paprd	dsafian	172.17.35.196	ROLE_EMPLOYEE	PY_IC_W4		
2017-08-16 09:57:01	hcprd	dsafian	172.17.35.196	ROLE_EMPLOYEE	PY_IC_W4	PY_IC_W4_DATA	EMPLID=7 7

Active Directory Lockouts

Active Directory Lockout Troubleshooting

Edit ▾

More Info ▾



Onyen

d*

Today ▾

Submit

Active Directory Login Failures

Account_Name ▾	AD Server ▾	Server on Which Failed Authentication Occurred ▾	Time ▾
skjeff	addc4	webdot0p	12/01/2016 04:10:43 PM

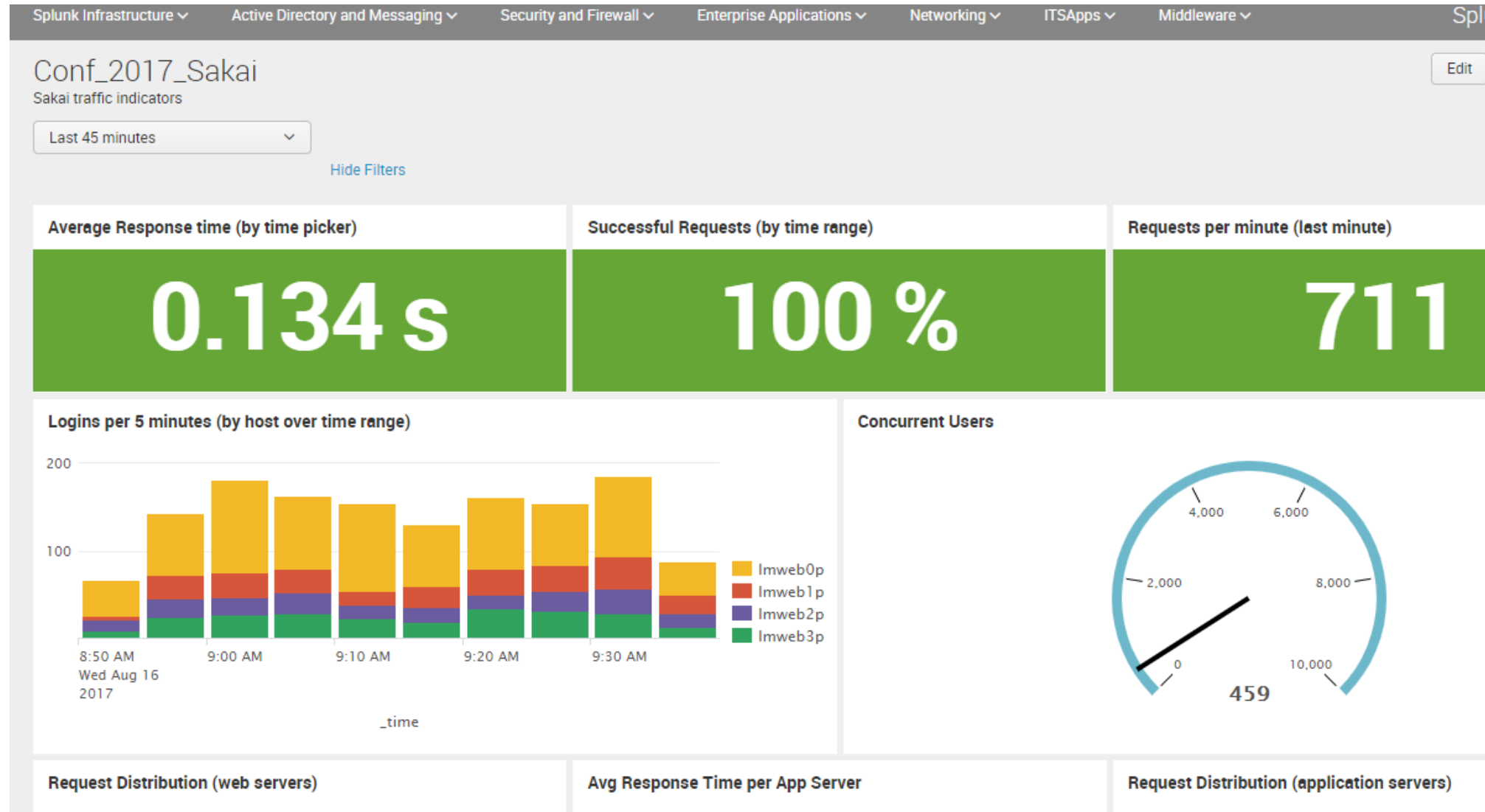
Exchange Login Failures

Time ▾	Account_Name ▾	Server on Which Failed Authentication Occurred ▾	Server Type ▾
12/01/2016 12:56:35 PM	arbones	ITS-MSXHT6F	Exchange SMTP
12/01/2016 12:56:12 AM	kimmiche	ITS-MSXCA1	Exchange Client Access

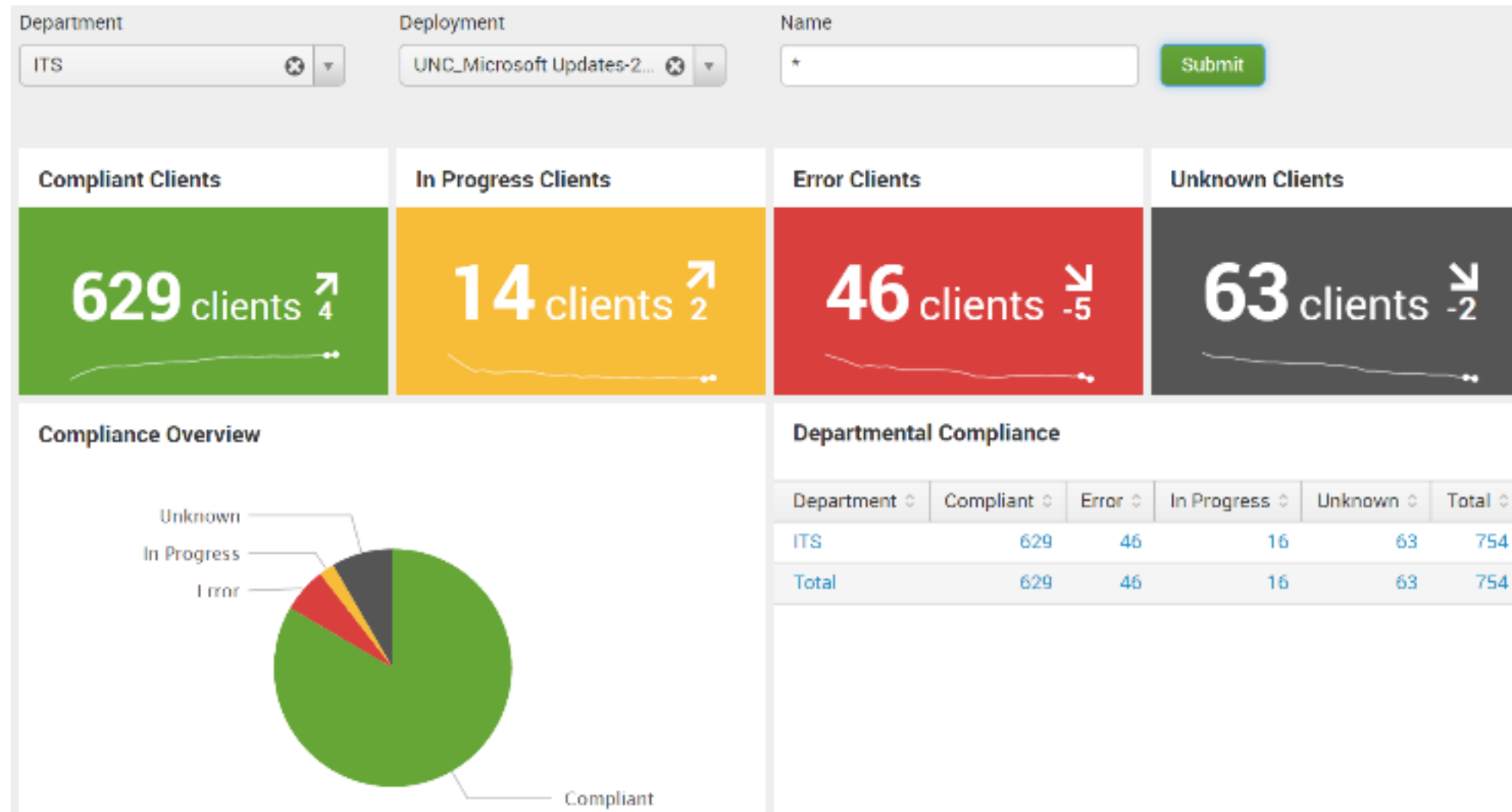
Direct Computer Login Failures

Time ▾	Account_Name ▾	Server on Which Failed Authentication Occurred ▾
12/01/2016 04:12:20 PM	jvmarcus	dhcp191069

Key Performance Indicators



Patching Compliance



Firewall Troubleshooting

Firewall Troubleshooting

Edit

Export ▾

...

Source IP Address

Destination IP Address

Destination Port

Firewall Action

Perform DNS Lookup

172.17.35.196

all

No

Time Range

Last 60 minutes ▾

Submit

[Hide Filters](#)

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 such as 152.19.250.* OR 152.19.250/24.

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:

Timestamp ▾	Action ▾	Firewall Address ▾	vsys ▾	Firewall Policy ▾	Src Address ▾	Src Zone ▾	dest_ip_c ▾	dest_zone ▾	Protocol ▾	dest_port ▾	Pkts In ▾	Pkts Out ▾	Session End ▾
2017/08/16 10:13:57	allowed	172.22.134.42	vsys6	ITSOSDMZP-0041	172.17.35.196	untrust	172.27.47.52	ITS-OS-DMZ-prod	tcp	8000	5	6	tcp-rst-from-client
2017/08/16 10:09:24	allowed	172.22.134.42	vsys6	MIDDLEWARE-0034	172.17.35.196	untrust	172.27.206.3	F5-DC-NoSNAT	tcp	443	10	9	tcp-fin
2017/08/16 10:09:24	allowed	172.22.134.42	vsys6	MIDDLEWARE-0034	172.17.35.196	untrust	172.27.206.3	F5-DC-NoSNAT	tcp	443	9	9	tcp-fin
2017/08/16 10:07:24	allowed	172.22.134.42	vsys6	MIDDLEWARE-0034	172.17.35.196	untrust	172.27.206.3	F5-DC-NoSNAT	tcp	443	10	9	tcp-fin
2017/08/16 10:07:24	allowed	172.22.134.42	vsys6	MIDDLEWARE-0034	172.17.35.196	untrust	172.27.206.3	F5-DC-NoSNAT	tcp	443	10	9	tcp-fin
2017/08/16 10:06:58	allowed	172.22.134.42	vsys6	MIDDLEWARE-0034	172.17.35.196	untrust	172.27.206.3	F5-DC-NoSNAT	tcp	443	10	9	tcp-fin
2017/08/16 10:01:58	allowed	172.22.134.42	vsys6	MIDDLEWARE-0034	172.17.35.196	untrust	172.27.206.3	F5-DC-NoSNAT	tcp	443	10	9	tcp-fin
2017/08/16 09:57:59	allowed	172.22.134.42	vsys6	MIDDLEWARE-0034	172.17.35.196	untrust	172.27.206.3	F5-DC-NoSNAT	tcp	443	10	9	tcp-fin
2017/08/16 09:57:14	allowed	172.22.134.42	vsys6	ERPD-1449	172.17.35.196	untrust	152.19.220.16	ERP-DMZ	tcp	443	9	10	tcp-rst-from-client
2017/08/16 09:57:14	allowed	172.22.134.42	vsys6	ERPD-1449	172.17.35.196	untrust	152.19.220.16	ERP-DMZ	tcp	443	11	12	tcp-fin

« prev

1

2

3

4

5

6

7

8

9

10

next »

Edit

Export ▾

...

Time Range

152.19.250.98

Last 30 days

Submit

Hide Filters

Firewall: Routing

Firewall search results:

Firewall: Host Vulnerabilities

Search results:

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

Q&A

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

Thank You

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

splunk> .conf2017