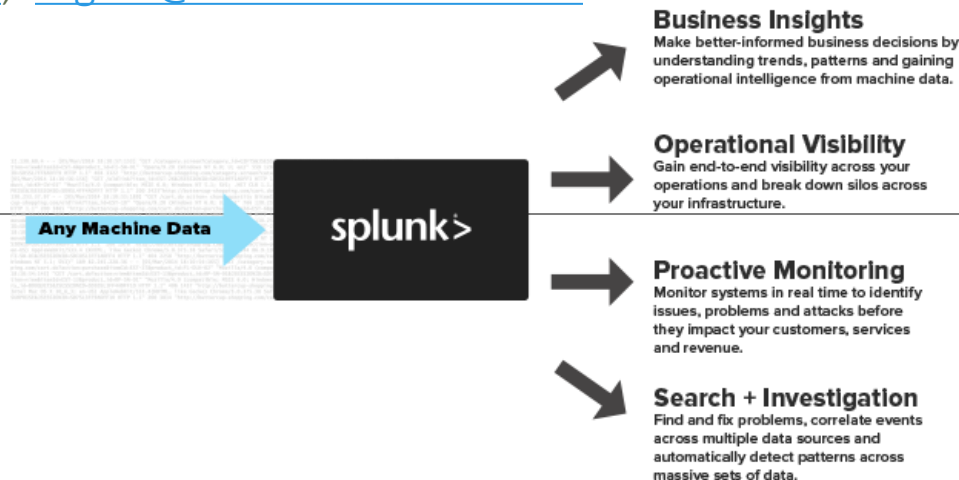


Turning Machine Data into Real-Time Insights

John Harper, Weijun Gao

harper@utsc.utoronto.ca, wgao@utsc.utoronto.ca

April 27, 2017



Outline

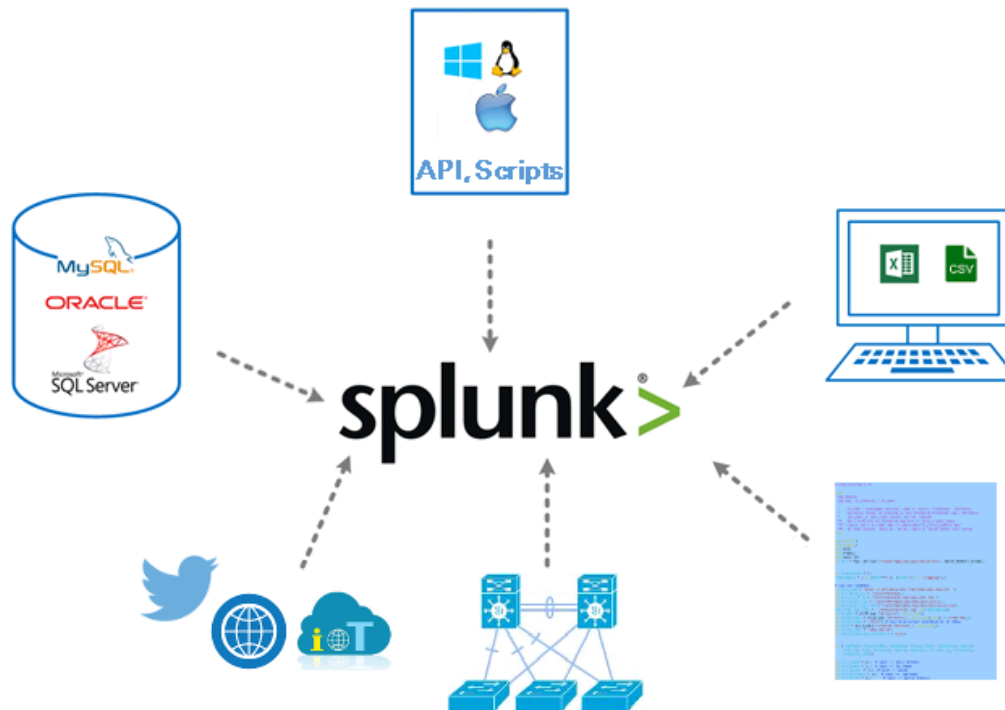
- Why Do We Need Splunk?
- Get Data into Splunk
- What Can We Do with The Data?
- UTSC Splunk Implementation
- UTSC Splunk Facts
- Use cases: Search, Analyze & Visualize
- Use cases: Dashboards
- Use cases: Anomalies
- Use cases: Alerts
- Use cases: Reports

Why Do We Need Splunk?

- Collect and index important machine data
- Retain and organize data
- Search and visualize data
- Generate alerts, reports from data
- Transform data for other software tools

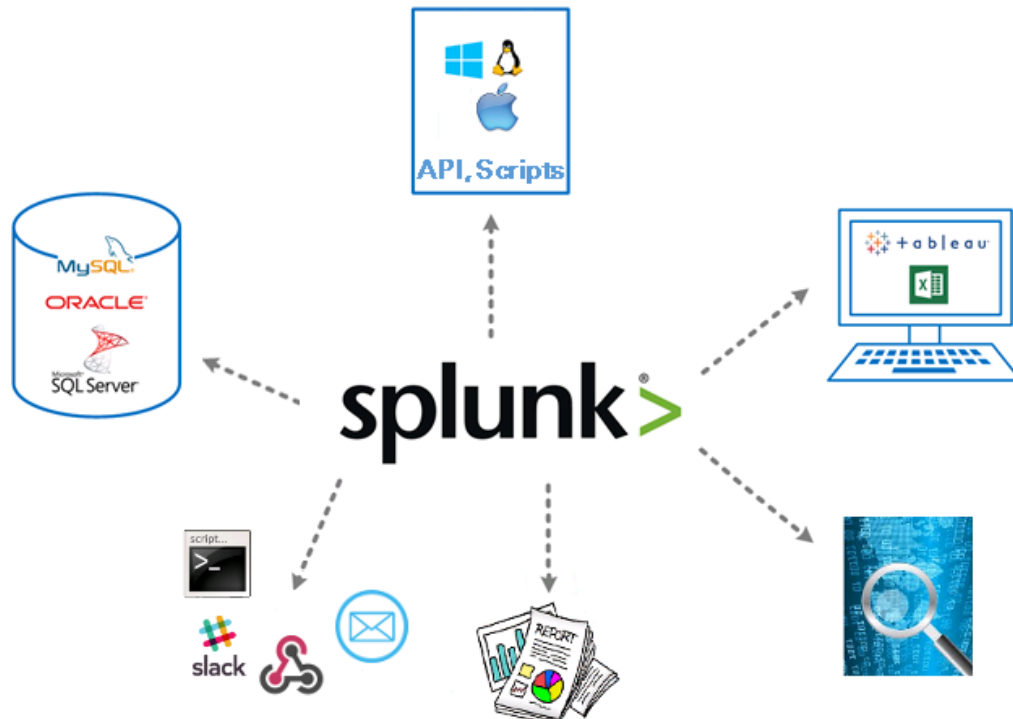
Get Data into Splunk

- * Text data
 - * Compressed text data
-
- Files and directories
 - Network streams
 - Scripted inputs
 - Lookup tables
 - Apps / Add-Ons

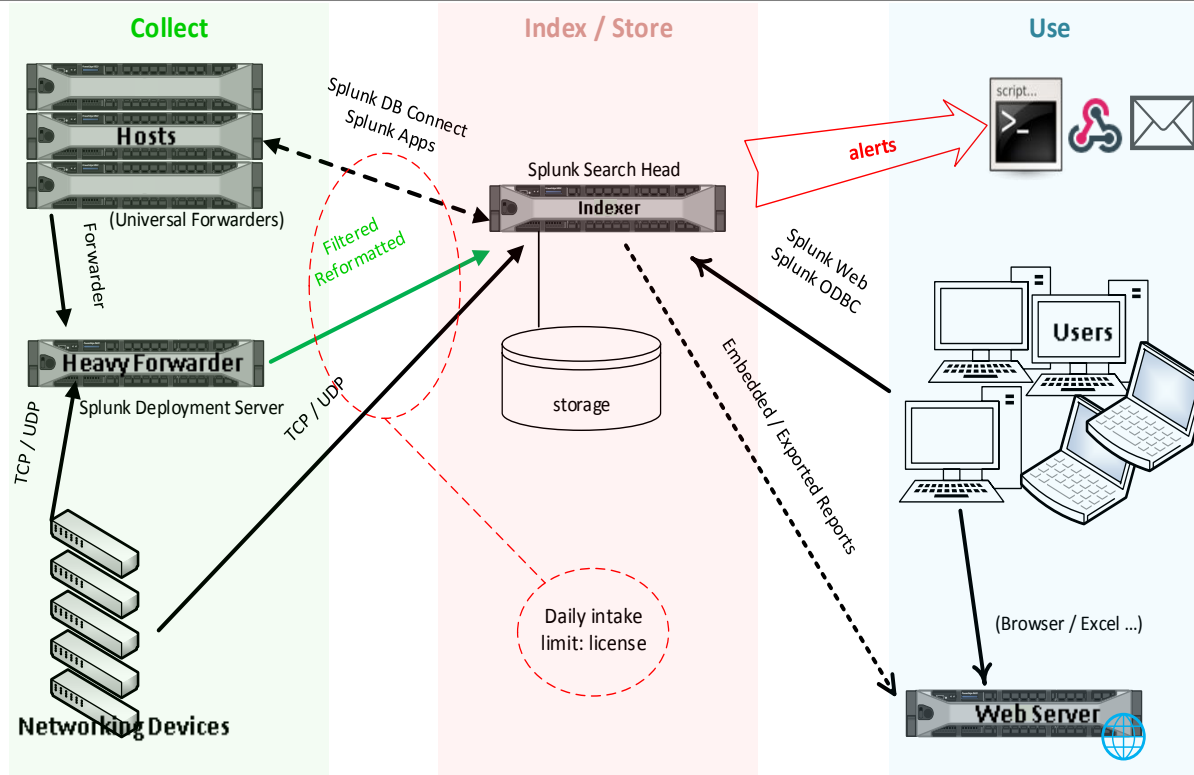


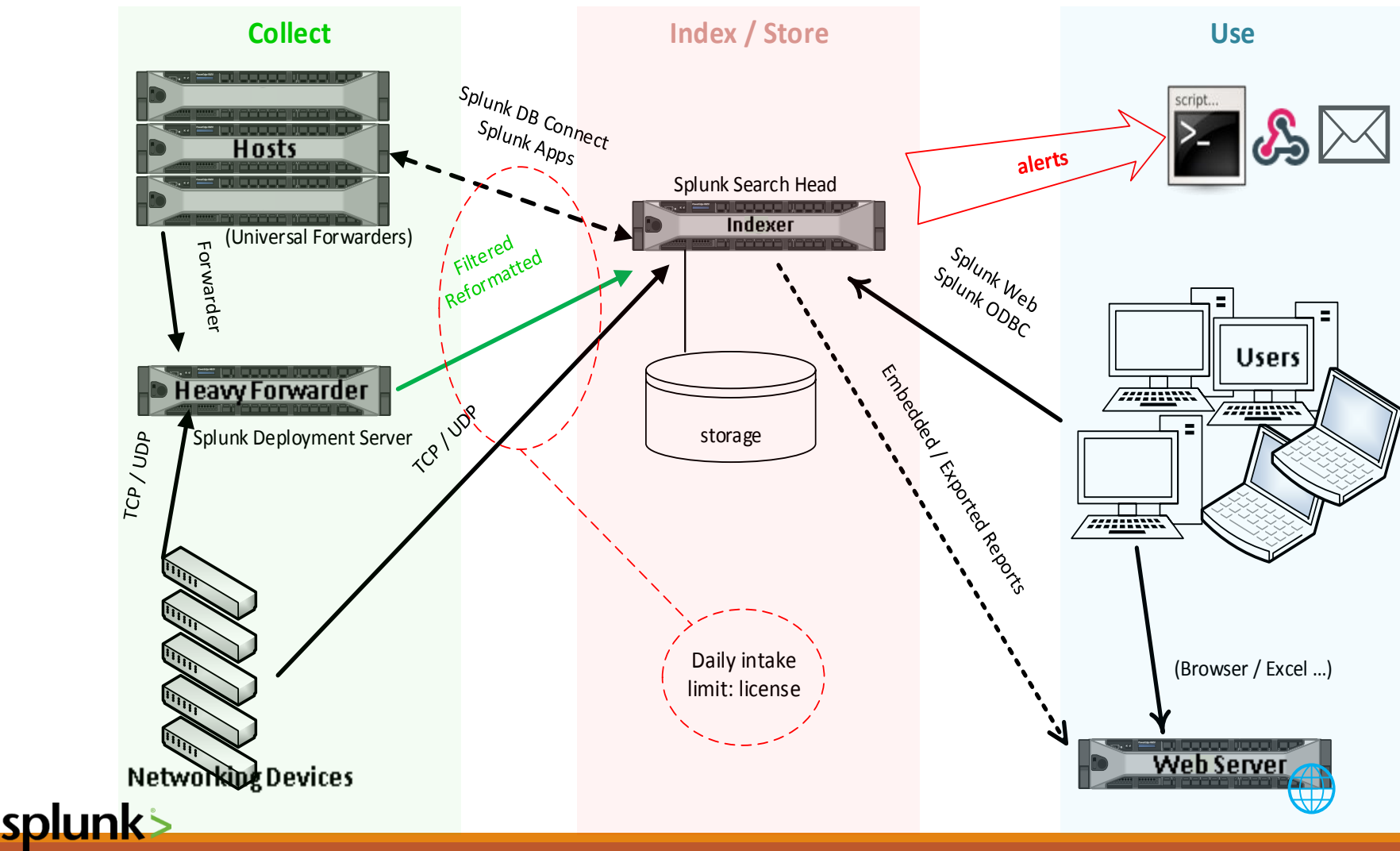
What Can We Do with The Data?

- Searching
- Statistics / Analysis
- Visualization
- Reporting
- Monitoring



UTSC Splunk Architecture



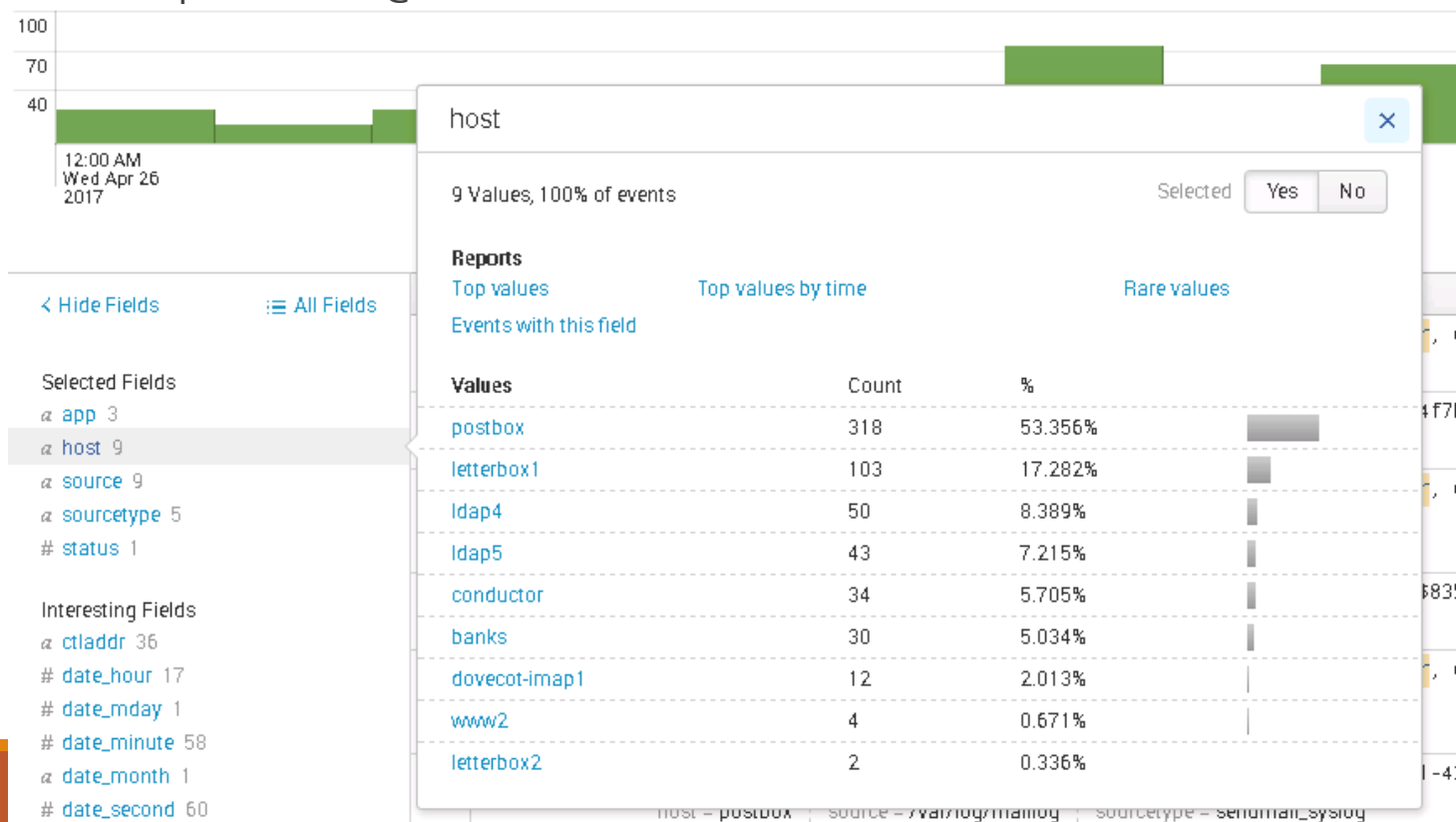


UTSC Splunk Facts

- Indexes 3 ~ 7 million events every day
- Collects data from ~100 networking devices and ~40 servers
- Logs of 60+ servers to be indexed in the near future
- Daily data intake is 0.5GB – 1.4GB
- License capacity: 2GB / day
- Heavy forwarder filters out 30 - 50% of collected events before sending to indexer
- Indexer (VM, debian): 16 CPU cores, 32 GB RAM
- Heavy Forwarder: 2 CPU cores, 4 GB RAM
- Storage: 300 GB used (2 years + historical data back to 2010)

Use cases: Search, Investigate & Visualize

➤ index=* harper earliest=@d latest=now



Use cases: Dashboards

UTSC Account Look up

To search 'user=<USERNAME>' in imap log, use search string: user USERNAME

To search 'user=<USERNAME>' in imap log and exclude 'XXXX', use search string: user USERNAME NOT XXXX

Input UTSCID or UTORID to search

Time Range

Today

select service

ALL

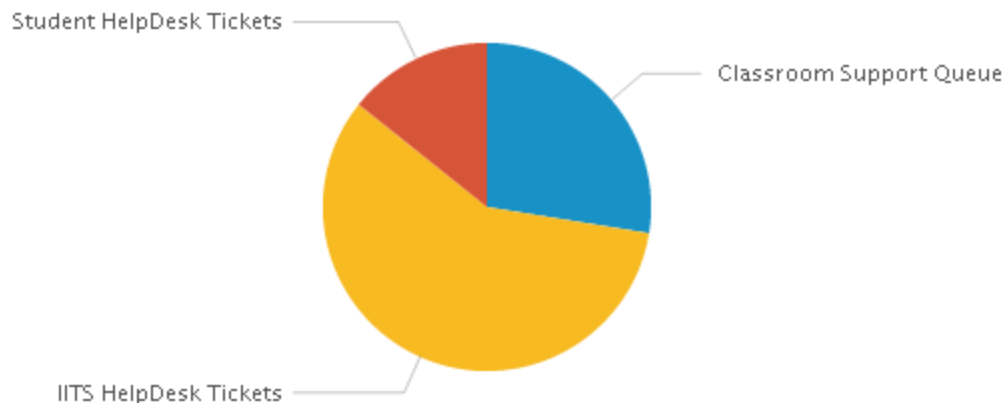
i	Time	Event
>	4/26/17 4:53:30.000 PM	Apr 26 16:53:30 ldap5 slapd[2899]: conn=14621858 op=2 BIND dn="uid=harper,ou=People,dc=uts
		host = ldap5 source = /var/log/ldap_details.log sourcetype = ldap
>	4/26/17 4:45:50.000 PM	Apr 26 16:45:50 letterbox1 sendmail[9889]: v3QKjFUE009869: to=<harper@utoronto.ca>
		host = letterbox1 source = /var/log/maillog sourcetype = sendmail_syslog
>	4/26/17 4:45:50.000 PM	Apr 26 16:45:50 letterbox1 dovecot: lda(harper): msgid=<E6CD4A07821704261645500000000000@letterbox1.utoronto.ca>
		host = letterbox1 source = /var/log/maillog sourcetype = sendmail_syslog
>	4/26/17 4:45:46.000 PM	Apr 26 16:45:46 letterbox1 huang: 2017/04/26 16:45:46 bureau85.ns.tion, not delayed by milter-greylist-4.5.12 (letterbox1.utoronto.ca)
		host = letterbox1 source = /var/log/maillog sourcetype = sendmail_syslog
>	4/26/17 4:42:59.000 PM	Apr 26 16:42:59 postbox sendmail[58726]: v3QKgsUn058723: to=harper@utoronto.ca
		host = postbox source = /var/log/maillog sourcetype = sendmail_syslog
>	4/26/17 4:42:59.000 PM	Apr 26 16:42:59 postbox dovecot: lda(harper): msgid=<038b01d2becd54425900000000000000@postbox.utoronto.ca>
		host = postbox source = /var/log/maillog sourcetype = sendmail_syslog
>	4/26/17 4:42:53.000 PM	Apr 26 16:42:53 ldap5 slapd[2899]: conn=14621541 op=2 BIND dn="uid=harper,ou=People,dc=uts

[Change History](#)
[Create Inputs](#)
[Data Model Audit](#)
[DHCP Exhaustion](#)
[Eventgen Logs](#)
[Eventgen Performance](#)
[Health & Wellness Firewall Dashboard](#)
[Logs](#)
[Orphaned Scheduled Searches, Reports, and Alerts](#)
[Overview](#)
[Predictive Analytics](#)
[Site Health Check](#)
[Status](#)
[Status History](#)
[Status Overview](#)
[TPASC WiFi User Counts of the Last 90 Days](#)
[UTSC - Radius authentication distribution - last 24 hours](#)
[UTSC Account Look up](#)
[UTSC CMS Lab Login Stats - 2016-12-05](#)
[UTSC CMS Lab Login Stats - last 120 days](#)
[UTSC CMS Lab Login Stats - yesterday](#)
[UTSC email sending and receiving](#)
[UTSC Email System Reports](#)
[UTSC Email System Summary Reports](#)
[UTSC failed ssh login attempts](#)
[UTSC HTTP-User-Agent Stats \(all sites\)](#)
[UTSC KACE tickets](#)
[UTSC Nextcloud stats](#)

Use cases: Dashboards

UTSC KACE tickets

Tickets - by queue



Tickets average open time in days - by queue

queue ▾

Classroom Support Queue

IITS HelpDesk Tickets

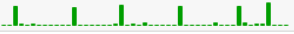
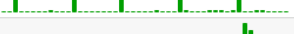
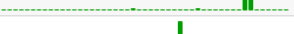
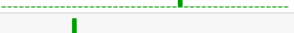
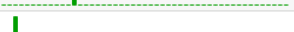
Student HelpDesk Tickets

Tickets Opened since 2013 - by month

500

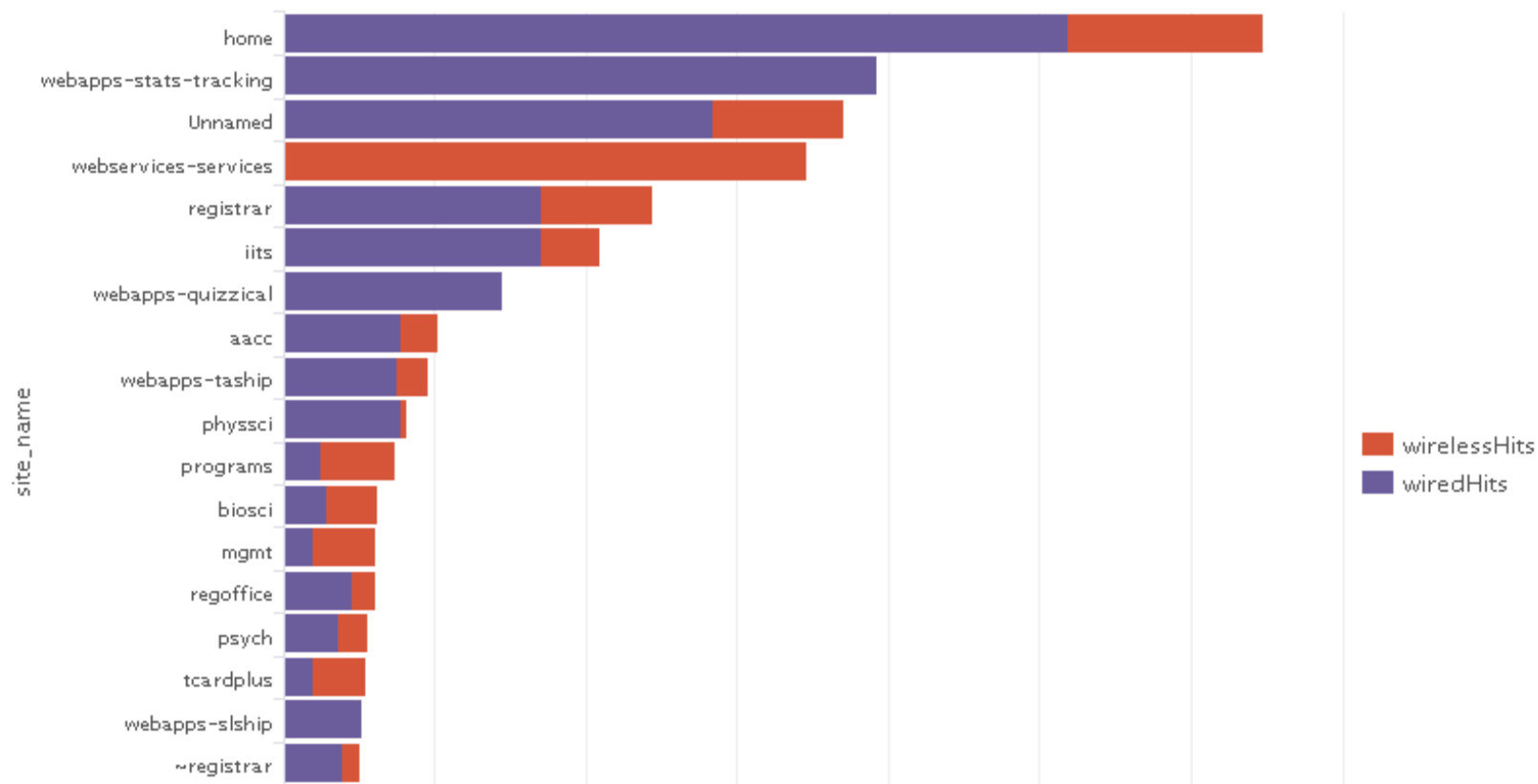
Use cases: Dashboards

Website Status

title ▾	url ▾	response_code ▾	last_checked ▾	response_time ▾	average ▾	range ▾	sparkline_response_time ▾
appstar	http://blog.utsc.utoronto.ca/appstar	▲ Connection timed out	2 minutes ago				
cps	http://www.apache.utsc.utoronto.ca:8000/~cps	▲ Connection timed out	just now				
clinical-psych	http://www.apache.utsc.utoronto.ca:8000/~psych/clinical-psych	▲ Connection timed out	4 minutes ago				
millerlashhouse	http://www.millerlashhouse.ca	● 200	3 minutes ago	672.15 ms	690.06 ms	633 - 845 ms	
aacc	http://www.utsc.utoronto.ca/aacc	● 200	3 minutes ago	22.60 ms	26.27 ms	21 - 748 ms	
aacc-contact	http://www.utsc.utoronto.ca/aacc/contact	● 200	5 minutes ago	63.53 ms	84.93 ms	62 - 937 ms	
aacc-cyp-guide	http://www.utsc.utoronto.ca/aacc/cyp-guide	● 200	just now	24.40 ms	37.38 ms	18 - 778 ms	
aboutus	http://www.utsc.utoronto.ca/aboutus	● 200	1 minute ago	20.70 ms	30.15 ms	18 - 664 ms	
academic-life	http://www.utsc.utoronto.ca/academic-life	● 200	2 minutes ago	23.21 ms	27.56 ms	19 - 479 ms	
acm	http://www.utsc.utoronto.ca/acm	● 200	3 minutes ago	26.29 ms	29.13 ms	23 - 478 ms	
admissions	http://www.utsc.utoronto.ca/admissions	● 200	3 minutes ago	23.48 ms	25.18 ms	21 - 47 ms	
anthropology	http://www.utsc.utoronto.ca/anthropology	● 200	4 minutes ago	322.84 ms	368.00 ms	308 - 1145 ms	
apply	http://www.utsc.utoronto.ca/apply	● 200	5 minutes ago	29.01 ms	34.49 ms	25 - 386 ms	
askcoop	http://www.utsc.utoronto.ca/askcoop	● 200	just now	24.01 ms	24.16 ms	18 - 375 ms	
athletics	http://www.utsc.utoronto.ca/athletics	● 200	2 minutes ago	23.59 ms	26.26 ms	20 - 763 ms	
biosci	http://www.utsc.utoronto.ca/biosci	● 200	3 minutes ago	24.04 ms	24.20 ms	19 - 520 ms	
businessdev	http://www.utsc.utoronto.ca/businessdev	● 200	just now	18.52 ms	23.63 ms	18 - 528 ms	
businessdev-exam-printing-form	http://www.utsc.utoronto.ca/businessdev/exam-printing-form	● 200	just now	64.13 ms	73.31 ms	59 - 389 ms	
businessdev-general-printing-form	http://www.utsc.utoronto.ca/businessdev/general-printing-form	● 200	just now	64.93 ms	74.80 ms	61 - 456 ms	
bythenumbers	http://www.utsc.utoronto.ca/bythenumbers	● 200	3 minutes ago	13.72 ms	31.00 ms	11 - 5019 ms	
campus-life	http://www.utsc.utoronto.ca/campus-life	● 200	1 minute ago	19.82 ms	25.46 ms	16 - 334 ms	
ccds	http://www.utsc.utoronto.ca/ccds	● 200	3 minutes ago	19.05 ms	32.58 ms	19 - 803 ms	

Use cases: Dashboards

top 20 most visited sites - UTSC users



Use cases: Dashboards

UTSC Email System Reports

Received Last 5 minutes

Email Count



Use cases: Anomalies

Sources with top log number changes

host ↕	source ↕	countsLastWeekDay ↕	countsToday ↕	countsRatio ↕
a2-ach1.netmgmt.utoronto.ca	udp:2514	8808	111	79.35
dovecot-imap2	/var/log/mail.log	1303	39642	30.42
a1-bv481a.netmgmt.utoronto.ca	udp:2514	4	120	30.00
cms4	/var/log/drupal/drupal_mslc.log	22	3	7.33
cms4	/var/log/drupal/drupal_hcs.log	28	4	7.00
cms3	/var/log/drupal/drupal_apply.log	26	4	6.50
142.1.96.8	udp:514	5662	36579	6.46
a1-bv487.netmgmt.utoronto.ca	udp:2514	87	549	6.31
a1-sl1a.netmgmt.utoronto.ca	udp:2514	1490	241	6.18
a1-ev4c.netmgmt.utoronto.ca	udp:2514	62	382	6.16
a2-sw5c.netmgmt.utoronto.ca	udp:2514	3927	651	6.03
a1-mw2s.netmgmt.utoronto.ca	udp:2514	36	6	6.00
cms3	/var/log/drupal/drupal_academic-life.log	23	4	5.75
a1-p3k.netmgmt.utoronto.ca	udp:2514	233	41	5.68
cms3	/var/log/drupal/drupal_research-innovation.log	22	4	5.50

Use cases: Alerts

Trigger Actions

+ Add Actions ▼

opens an issue in JIRA



Log Event

Send log event to Splunk receiver endpoint



Run a script

Invoke a custom script



Send email

Send an email notification to specified recipients



Slack

Send a message to a Slack channel



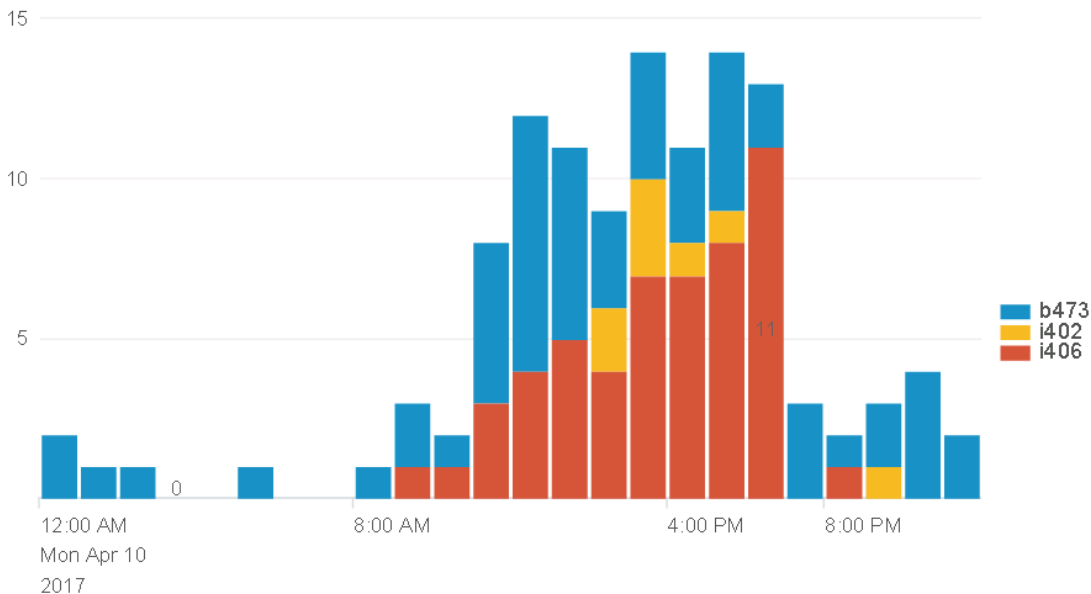
Webhook

Generic HTTP POST to a specified URL

[Manage Alert Actions](#)

- > CPU_Under_Percent_by_Host
- > Cisco 4500 Temp Alarm
- > DHCP no free leases
- > Disk_Used_Exceeds_Perc_by_Host
- > IO_Utilization_Exceeds_Threshold
- > IO_Wait_Exceeds_Threshold
- > Idrac fault
- > Load_Exceeds_by_Host
- > Memory_Exceeds_MB_by_Host
- > Memory_Exceeds_MB_by_Process
- > Memory_Exceeds_Percent_by_Host
- > Missing wireless radius config
- > Open_Files_Exceeds_by_Process
- > Processes_Exceeds_by_Host
- > Res AP Down
- > Threads_Exceeds_by_Host
- > UTSC-Nextcloud-free-disk-space-is-less-than-100GB
- > UTSC-Nextcloud-login-failed
- > UTSC-Nextcloud-users-quota-usage-reached-90%
- > UTSC-ad-accounts-locked-out
- > UTSC-critical-idrac-message(s)
- > UTSC-hourly-DHCP-syslog-count-reached-175000
- > UTSC-new-watchdog-target(s)-created
- > UTSC-per-ip-per-5m-404-hits-over-20-times
- > UTSC-watchdog-scan-stopped
- > UTSC-website-error
- > WLC Radius Auth Server Failure
- > We have eduroam zombies!
- > Wi-Fi DFS Channel Alert

Use cases: Reports



UTSC - MSSQLL Login Report - utscbim - failed - last 30 days
UTSC - MSSQLL Login Report - utscbim - failed - today
UTSC - MSSQLL Login Report - utscbim - failed - yesterday
UTSC - MSSQLL Login Report - utscbim - succeeded - last 30 days
UTSC - MSSQLL Login Report - utscbim - succeeded - today
UTSC - MSSQLL Login Report - utscbim - succeeded - yesterday
UTSC - TPASC WiFi average unique user counts by weekdays
UTSC - TPASC WiFi daily unique user counts
UTSC - TPASC WiFi daily unique user counts list
UTSC - utscbim MSSQLL Login Report - succeeded - last 30 days
UTSC-cms-labs-term-report
UTSC-dhcp-no-wireless-results-last30days
UTSC-www-per-ip-per-min-hits-greater-than-250
UTSC-www-per-uri-per-min-hits-greater-than-150
utsc_drupal_sites_failed_access_last7days
utsc_error_counts_today
utsc_nginx_PageHits_NoImages_last30days
utsc_nginx_PageHits_NoImages_today
utsc_nginx_PageHits_last30days
utsc_nginx_PageHits_today
utsc_nginx_UriStaRef_search_today
utsc_nginx_referer_search_last30days
utsc_nginx_referer_search_today
utsc_nginx_ua_search_today

Use cases: Embed or Export

Secure | <https://splunkreports.utsc.utoronto.ca>



Home @ UTSC Splunk Reports Site

Available Reports

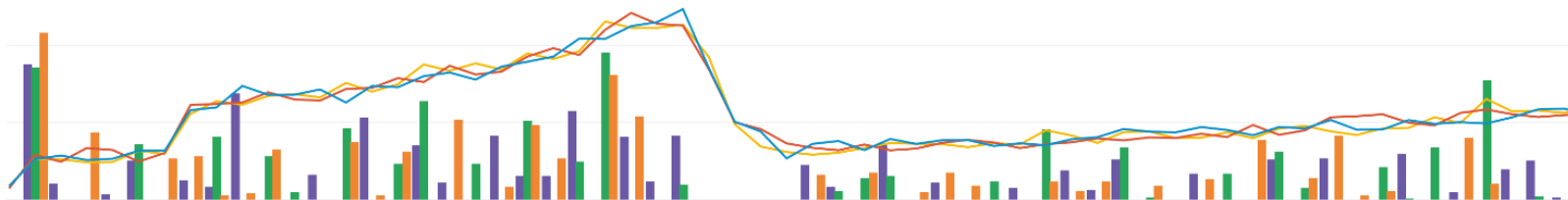
[cmslabs](#) | [mssql](#) | [nextcloud](#) | [watchdog](#)

For users:

Most of the reports are protected, if your UTSC login doesn't work, ask [UTS](#) Systems group (systems at utsc dot utoronto dot ca).

To sign out after you sign in, click on a **Sign out** link and then click on "Cancel" button when a login dialog pops up. For some browsers, you may need to exit your browser to sign out completely.

You may need to wait for up to a few minutes for new report(s) to be created after you click on "create_a_new_report.php" or "create_new_reports.php" if one is provided.



For internal developers:

This website hosts exported Splunk dashboards (PDF files) and embedded Splunk reports. Dashboard PDFs can be automatically exported once configured on UTSC Splunk Server ...

The following script can be used as a template to create a page for embedded reports (PHP, index.php, for example):

```
<?php /* set the page title */ $GLOBALS['title'] = 'UTSC Splunk Reports'; ?>
<?php /* display today's date or not */ $GLOBALS['showDate'] = true; ?>
```

Use cases: Splunk ODBC

Book1 - Excel

Review View Tell me what you want to do...

Queries Table Data Sources Transform

Connections Refresh All Properties Edit Links

Sort Filter Clear Reapply Advanced

Text to Columns Flash Fill Remove Duplicates Data Consolidate Relationships Manage Data Model What-If Analysis

Navigator

Select multiple items

Display Options

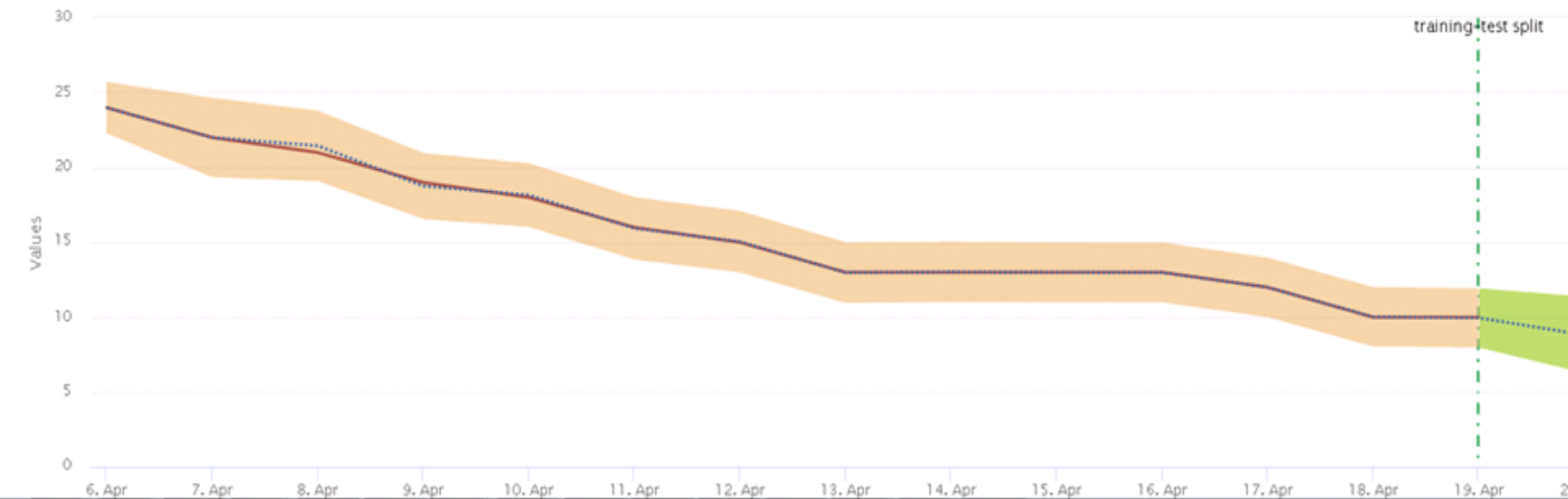
- utsc_nginx_PageHits_NoImages_last30d...
- utsc_nginx_PageHits_NoImages_today
- utsc_nginx_PageHits_today
- utsc_nginx_referer_search_last30days
- utsc_nginx_referer_search_today**
- utsc_nginx_ua_search_today
- utsc_nginx_UriStaRef_search_today
- UTSC-ad-accounts-locked-out
- UTSC-cms-labs-term-report
- UTSC-critical-idrac-message(s)
- UTSC-dhcp-no-wireless-results-last30days
- UTSC-GPA-calculator-2015
- UTSC-GPA-Calculator-Monthly

utsc_nginx_referer_search_today

referrer	totalCount
-	28555
https://www.google.ca/	5991
https://www.google.com/	734
http://www.utsc.utoronto.ca/home/	468
http://www.utsc.utoronto.ca/	353
https://www.google.co.in/	259
http://www.utsc.utoronto.ca/registrar/	188
http://www.utsc.utoronto.ca/~residences/townhouses.html	163
http://www.utsc.utoronto.ca/registrar/contact	161
http://www.google.ca/	146
http://www.utsc.utoronto.ca/administration.html	138
https://www.google.co.uk/	138
http://www.utsc.utoronto.ca/programs/utscfood/	117
https://www.google.com.vn/	114
http://www.utsc.utoronto.ca/~registrar/scheduling/timetable	113
https://www.google.com.hk/	105

Use cases: Prediction

Forecast [🔗](#)



Free Resources

- Splunk Pledge – free, 10GB/day, one year, for research and teaching purposes
https://www.splunk.com/en_us/about-us/splunk-pledge.html
- Free 500 MB/day License
https://www.splunk.com/en_us/download.html
- Free Splunk Training – starts in May, requires an @utoronto.ca E-mail
<https://www.canarie.ca/members/splunk/>
Caglar Ulugbay – culugbay@splunk.com
- Free Splunk eBook
<http://www.splunk.com/goto/book>

Thank you!

Questions?

E-mails: harper@utsc.utoronto.ca, wgao@utsc.utoronto.ca

Slides: <http://splunkreports.utsc.utoronto.ca/tkf17>