



.conf2015

Making Splunk Your Primary Information Portal

Splunk Dashboarding in Action

Donald Mahler

Performance Engineering and
Systems Monitoring, Leidos

splunk®

Disclaimer

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. Referenced customers for ITSI product participated in a limited release software program that included items at no charge.

Who We Are

- Science and technology solutions leader
- Focus on national security, health, and engineering
- Government and commercial customers
- Created 9/27/13 and headquartered in Reston, VA



*Leidos Leadership at the New York Stock Exchange
Ringing the Opening Bell*

Who Am I ?

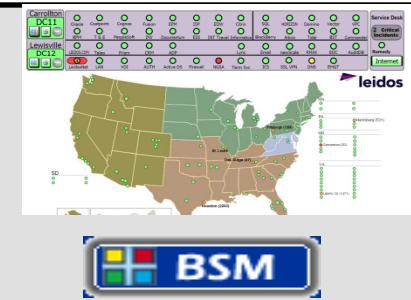
- Director of Performance Management/Monitoring at Leidos, a science and technology solutions leader, based in Reston, VA
 - Internal Leidos IT include business service management (BSM), server/cloud monitoring, application performance, and common security/network/application logging
- Career in systems/network management across many platforms and OS's; presented at numerous conferences and seminars on technology and solutions
 - 2014 Splunk .conf and Gartner infra ops conferences
 - SplunkLive events (in NYC and DC)
 - Aprisma Spectrum user conference (keynote), Netiq's Netconnect, Novell's BrainShare, Managed Object's user conference, IBM AOTC, Planet Tivoli, IBM SHARE.

Agenda

- Our original portal and philosophy
- Overview of our Splunk core environment
- The rise of Splunk usage
- Splunk for Dashboarding

Operational Intelligence

Situational Awareness



Performance and Capacity Reporting



Common Logging and Analysis



splunk™

Network Management

- Collaboration w/ ITSM and monitoring
- Alerting/ ticketing/dispatch on production issues
- Correlation of issues to the effect on the business IT services

Server Management

Infrastructure Management

Application Mgt and Synthetics

ITSM integration (ticketing, change, CMDB)

- Dashboarding and reporting
- Performance and inventory reporting
- Infrastructure-wide logging

Monitoring Products

EMGTweb



Business Service Management (Netiq Operations Center)

Network Management

Server Management

Synthetics

NPM

OEM

ipMonitor

Cascade
Netflow

Exchange

Splunk Windows

WPM

HP NA

Lync

Active Directory

F5

Appmanager

Batch Services

Vcops/ vCenter

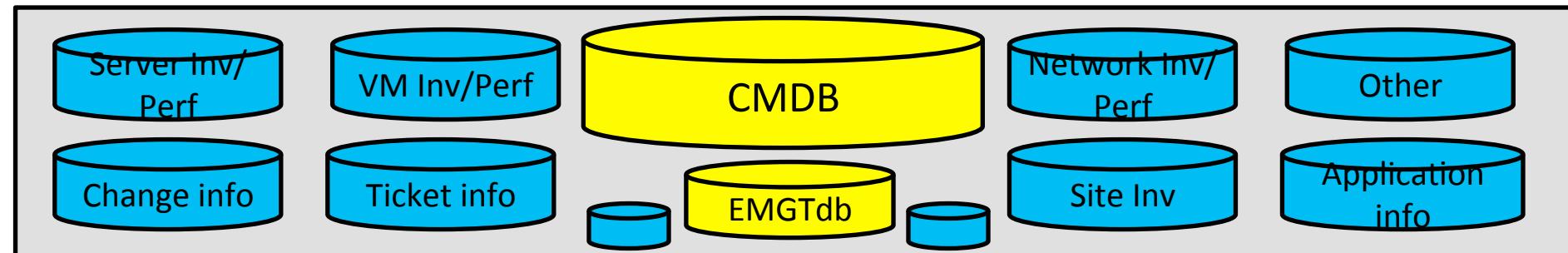
Backups

HPSim

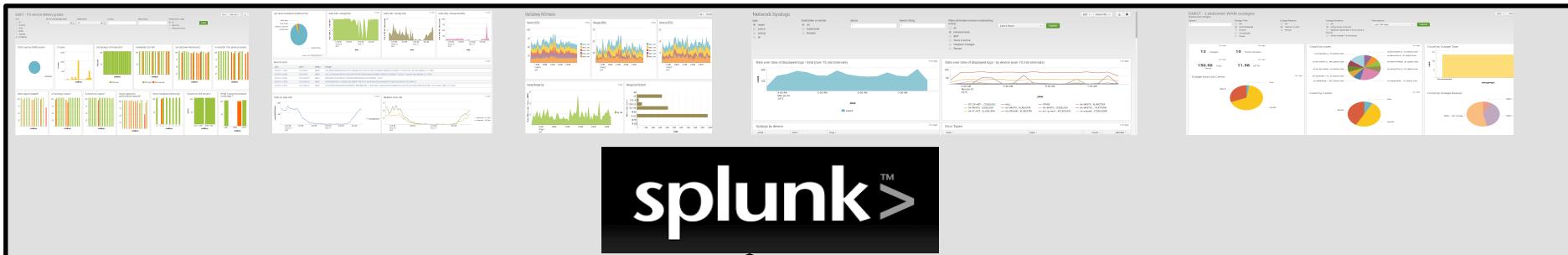
Splunk

ITops Reporting Sources

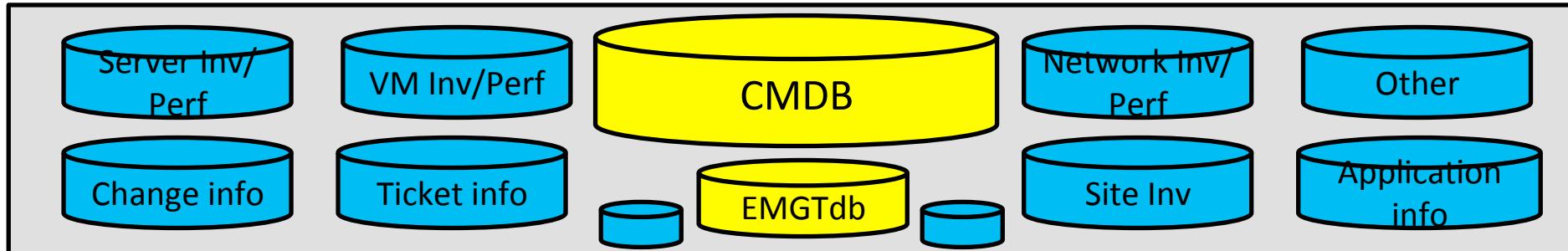
- ITIL— all services rooted in the CMDB
- Report on services from various sources (in context)
 - Already had access to all this
- The insight comes from when you combine the towers
 - Example: correlating monitoring with ITSM ticket/change



Splunk - Atop the Management Ecosystem



Logfiles, Agents
Dbconnect
Dbquery
CSV



What is IT Operational Reporting?

- The need to know the state of the enterprise, across many dimensions
 - Status – including monitoring, ticketing, changes
 - (what we think is happening, what the users think, what we have changed)
 - Problem investigations (what did we know and when?)
 - Inventory
 - Performance
- Common portal access - Provide lots of varied content up and down the stack
 - From Switch port usage to ticket rates, to WAN circuits, all the way to overall service status

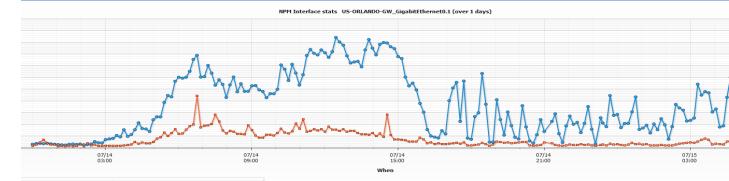
In general, we need to show and tell: list things, graph them over time, highlight anomalies, etc....

EMGT and EMGTweb

- Hand crafted / HTML based - originally circa 2000
- Displaying information from various monitoring DB's
 - Underlying heterogeneous CMDB/ inventory DB – emgtDB
 - Accesses product DB's
- HTML
 - Tables- color cells , raw scripting, with some ASP
- Cumbersome web development and adding of features
 - Time selection
 - Wide variety of interface "feels"
- Anychart for graphing

The screenshot shows the EMGT web interface. On the left is a sidebar with links: BSM, ServiceDelivery, Tickets, Performance, Inventory, Logfiles, and ContactDB. The main area has tabs: Status, Tickets/RFCs, Service Delivery, MyEMGT, Special Reports, Inventory, Monitoring, Splunk, Consoles, OSC Tools, and Notification. A search bar is at the top. The central part displays a ticket list with columns: Item, Type, Impact, Downtime Timeline, Details As of, and Resolution. One ticket is highlighted in yellow.

Clearly we needed to do something



Our Splunk Journey

- Pre 2010
 - Syslog servers (“tail and spit”)
- 2010 – Splunk 10GB
 - Routers, switches
- 2012 – Splunk 400GB
 - Router, switches, Firewalls, Servers
- 2013-2014 - bump to 700GB/day (then split company 400/300)
 - More servers, more networking gear , more applications



What is in our Splunk?

- Over 2,000 devices send data to Splunk
- Splunk consumes up to 400GB of logging and performance data daily
- Feeds alerts, ticketing, changes, performance data

DB: database

DNS: Domain Name Service

DHCP: Dynamic Host Configuration Protocol

VPN: Virtual Private Network

IDS: intrusion detection system

IPS: Intrusion prevention systems

SSL: Secure Sockets Layer

WIFI: wireless fidelity

VMware is a registered trademark of VMware, Inc. in the U.S. and/or other countries.

Active Directory and Windows are registered trademarks of Microsoft Corporation in the U.S. and/or other countries.

Linux is a registered trademark of Linus Torvalds in the U.S. and/or other countries.

Auth	Active Directory®	SSL VPN
	Firewall	Proxies
Security	IDS	IPS
	Switches	DNS/DHCP
Network	Routers	WIFI
	VMware®	Windows®
Computing	Physical	Linux®
	Monitoring	Web/DB Logs

What Splunk Brings to the Table

- It has all the data
 - Ability to consume all the information (logs/collectors/Dbconnect)
 - Or reach out and grab it as needed (dbquery)
 - *New mindset – gather the data and figure out a use for it later*
- Common look and feel
 - Ability to build out selection criteria (even using dynamic criteria)
 - Nice widgets to make the dashboarding more compelling
 - Shared concept of time
- Powerful graphing
 - Graph everything the same way, whether it is server cpu, user response time, router link utilization
 - Quick reframing of time



Share the data, free the people

Along Comes Splunk 6

- Easy XML dashboarding
- Dashboard editing
- Smart drilldown
- Easy prototyping
- Use of timed data
- Use of lookups



".conf session on dashboarding"

EMGT2 - The ITO Reporting App in Splunk

- Are we delivering quality IT services?
- How's our availability? What's happening right now?
- What happened last night? Last week?
- When was that server last rebooted
- Did the backups work?
- Did the batch jobs run? How long did they take?
- Any red flags in our Lync servers? How bad are the call quality MOS scores?
- Who is that server talking to? Is it being denied?

Currently 80+ dashboards and 30+ legacy links

Status/Performance ▾

ITSM: tickets/changes/onCall ▾

Inventory/CMDB/Grades ▾

Network ▾

Service Dashboards ▾

Explore ▾

Tools ▾

EMGTweb ▾

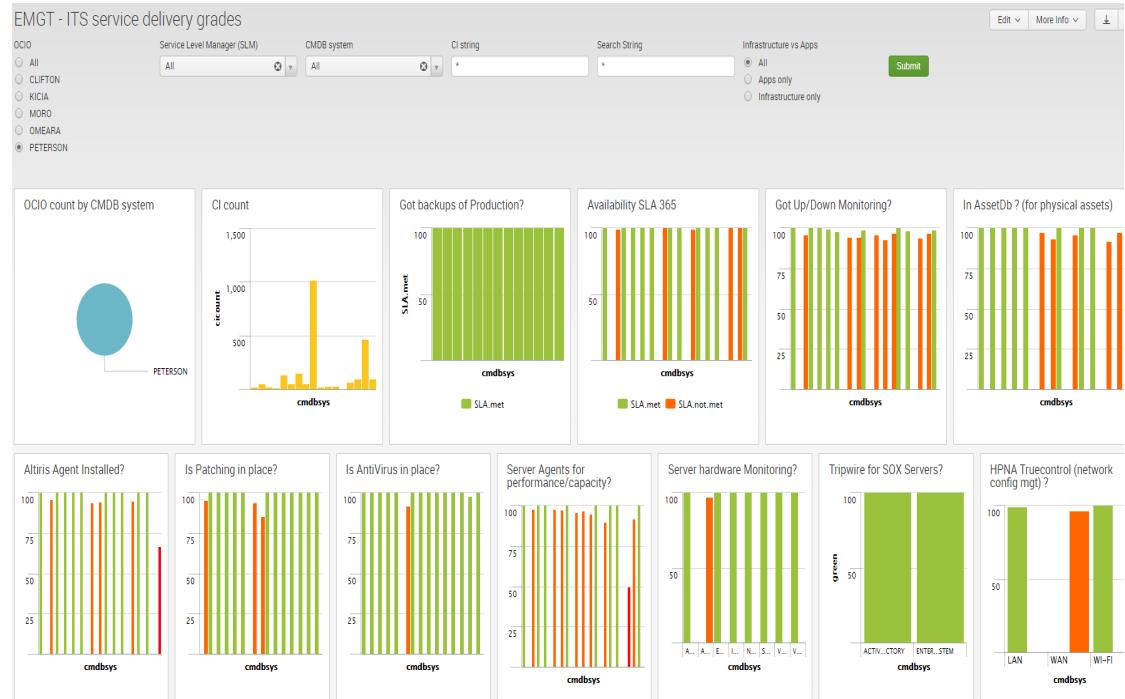
Dashboards

search

.conf2015

Step 1 – Get Requirements

- Define the need, users, security
- Who is the audience?
- Is it appropriate?
- Do we have the data we need?
- What types of insights are we looking for?
- What happens on drilldown? (where do you want to take them)



Step 2 – Gather Your Data

Logfiles

- Syslogs
- Router/switch logs
- App logs
- Authentication logs
- Firewall logs

Classic logfile data

DB connections

- Network util, CPU
- Server metrics
- App metrics
- Synthetic metrics

Time-series structured DB queries

Lookups

- CMDB
- Network inventory
- AD user/computer info
- Altiris PC info

Status/refreshed CSV

Dbquery

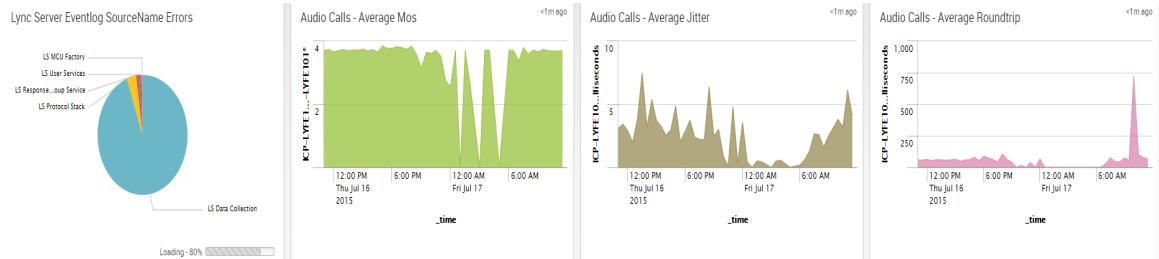
- BSM
- Availability reports information

External realtime DB queries

Step 3 – Design the Dashboard

Purpose

- Targeted purpose (like status displays)
- Inventory vs history
- Explorers



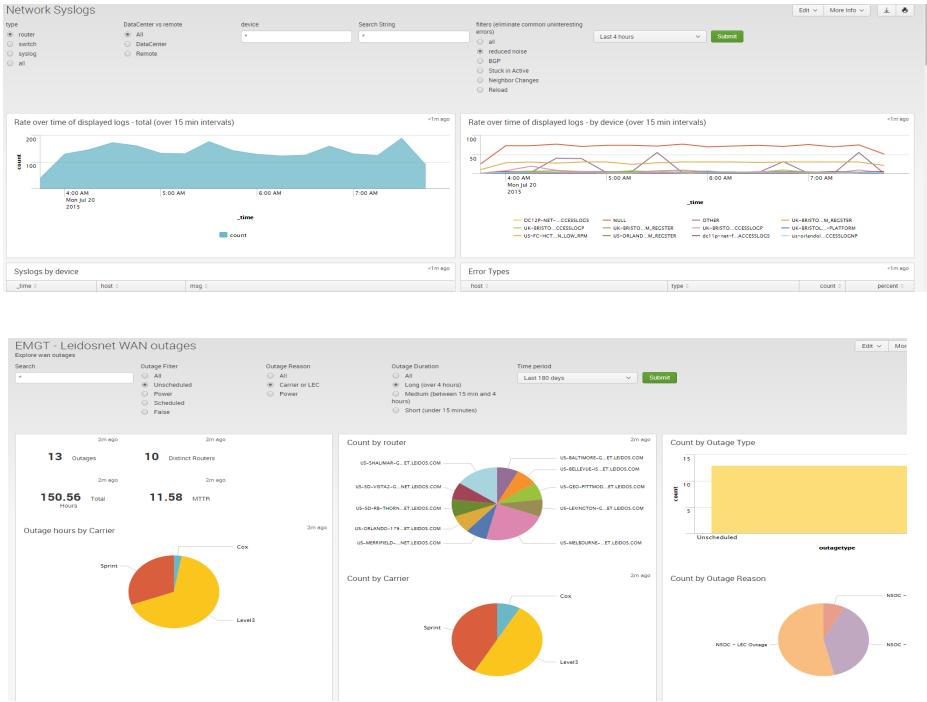
Decide on widgets

- Tables, graphs, column/bar/pie charts, single values
- Prefer highly dense dashboards
 - Rows and panels



Step 4 – Publish and Iterate

- Rapid development and updates
- Anchor into menu
- Examples:
 - Syslog analysis, while issue was happening
 - Network outage reports, to quantify reimbursement requests



EMGT2 – Splunk App - Structure

- **Status**
 - Across the board perspectives, including a summary page
 - Performance highlights and hot spots
- **ITSM**
 - Ticketing, changes, problem
- **Inventory**
 - Systems/Services, CMDB, various inventories, counts
 - Service delivery grades
- **Network**
 - Sites, inventory, alerts, performance, syslogs
- **Service** – hand build views
- **Explore**
 - Myriad of areas, including batch jobs, backups, service accounts, inventory
 - Server, synthetic, network performance
- **Tools**
 - Firewall log queries, syslog searches, alert searches
- **EMGTweb** – misc links
- **Dashboards**
- **Search**

Status: Landing Page – What's Going On?

- Is anything hot right now?
 - Sev1 tickets, ticket flow, BSM
 - Major alerts, major changes
 - Spiking routers and servers

The screenshot displays the Splunk Status: Landing Page with several open panels:

- EMGT - Overall Status**: A dashboard showing critical and high priority tickets from various sources like NOC, BPM, Telecom, and Network.
- Tickets - Incoming Flow (last 60 minutes)**: A table showing the count of incoming tickets categorized by type (Enterprise Applications, Desktop OS, Desktop Software, User Administration, Telecom, Email, Network, Network Security, Server, Database).
- BSM service log**: A log table showing recent events with columns for time, service, and severity (e.g., OH, ISF, ISP).
- Backup Issues (last 24 hrs)**: A list of backup jobs and their status (e.g., ISPP-ISP04 ISF, ISPP-ISP03 ISP, ISPP-ISP02 ISP, ISPP-ISP01 ISP, IDPP-SECUTLL04 INTRUSION DETECTION AND PREVENTION, SQLP-DB02 ENTERPRISE DATABASE, SQLP-DB01 ENTERPRISE DATABASE, ORDBP-10 ENTERPRISE DATABASE).
- Click to see TECweb in Splunk**: A table of active alerts with columns for time, host, severity (CRITICAL), and message (e.g., CPU UTILIZATION IS HIGH TOTAL CPU PROCESSOR TIME IS AVERAGING 100.0 OVER THE LAST 45 MINUTES SPLUNKAGENT SPLUNK NBU-SUP01 NBUP-SUP01).
- All RFCs (drilldown available to full RFC details)**: A table of RFCs with columns for time, rfc.no, request.title, implementation_group, requester_name, and request_. (e.g., 2015-07-14 10:00:00, 0000046008, Security appliance/server maintenance restart & reboot (CoreWare), NetSecEng, May, Daniel A, Intrusion and Prev).
- Click to see all "what changed" information**: A table of what-changed information with columns for time, rfc.no, request.title, implementation_group, requester_name, and request_. (e.g., 2015-07-13 18:00:00, 0000046000, SIERRA-SECOPS SIERRA Support - MAY, DANIEL A, Leiden University Integration, IISBU SecOps, Thavone, Phaihoun, Firewall).
- 2015-07-13 08:00:00**: A row of what-changed entries for a specific event (e.g., 0000045986, WinAdmin-mandatory enterprise applications or software (Please get Admin installed on Domino servers as it's failing), EC-Windows Admin, Roman, Randy, Desktop).
- 2015-07-13 03:00:00**: A row of what-changed entries for a specific event (e.g., 0000046002, IISBU-SECOPS SIERRA-9726 Support, IISBU SecOps, Rudick, John W, Firewall).
- 2015-07-12 14:00:00**: A row of what-changed entries for a specific event (e.g., 0000045991, Log4j - Production outage Getting ADAM error, EC-Windows Admin, Treeman, Eric M, Cognos).

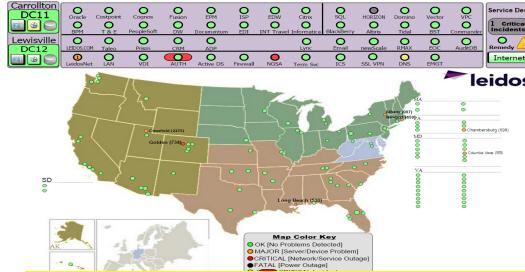
Status: What Changed?

- First thing asked when major issues happen
- Put all views of “change” in one place
- **How:**
 - *Pull in all view's of change into one dashboard*
- Approved Request for Change
- RFC suppressions
- Network config changes
- Firewall changes and content changes
- Reboots (network / server)
- Altiris installs
- Tripwire

All RFCs (drilldown available to full RFC details)							3m ago
_time	implementation_group	request_title	rfc_no	requester_name	request_subcategory	request_type	
2011-01-01T00:00:00Z	Implementation Group A	Request Title A	12345	User A	Category A	Type A	

Status: Critical Alerts and BSM

- How are we doing right now
- Alert perspective vs BSM perspective
- *How:*
 - *Dbquery to BSM / manager of managers DB*
 - *Drilldown based on column*



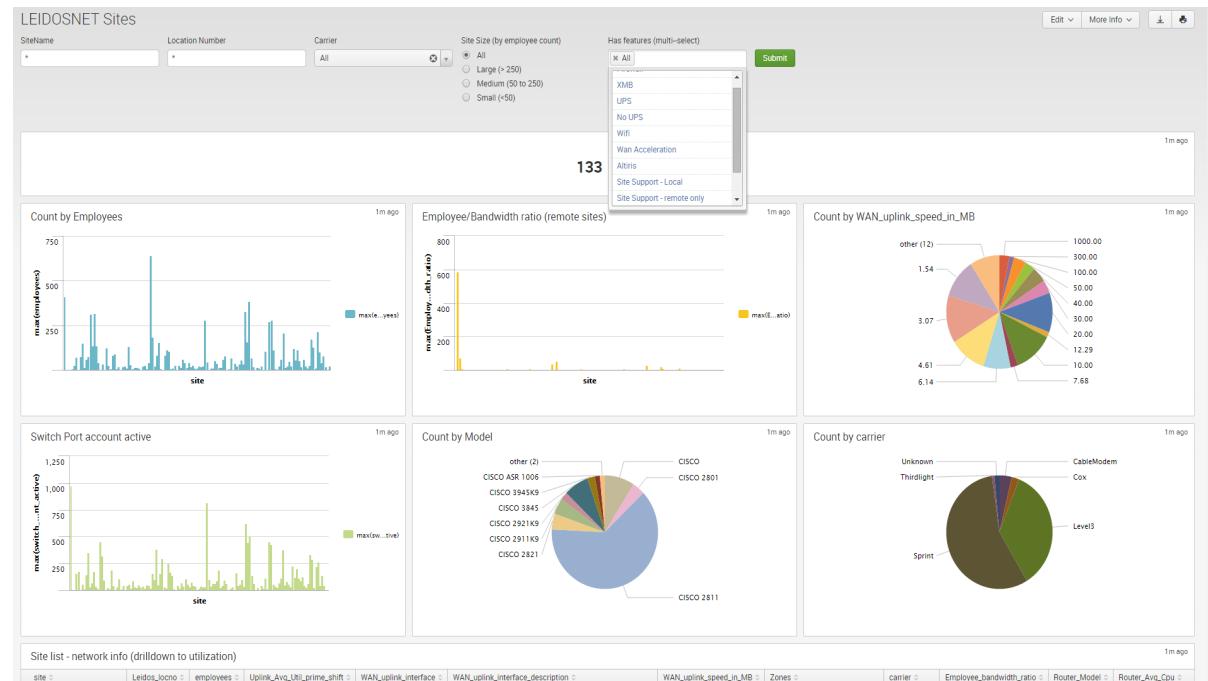
BSM service log

_time	service	severity
2015-07-27 12:45:51	BPM	OK
2015-07-27 11:32:38	LeidosNET	Minor
2015-07-27 02:04:10	Strong.Authentication	Critical
2015-07-26 20:25:39	Enterprise.Database.System	WN
2015-07-26 19:01:33	BST	OK
2015-07-26 12:05:02	Domino	OK
2015-07-25 05:40:38	Workday.Functional	OK
2015-07-25 05:09:57	Altiris	OK

```
<drilldown target="_blank">
  <link field="host">
    <![CDATA[
      /app/EMGT2/emgt_simple_log_search?form.searchstring=$row.host$]]>
  </link>
  <link field="status">https://externallink1?$row.eventkey$_$row.host$</link>
  <link field="time"> https://externallink2?$row.eventkey$</link>
  <link field="severity"> https://externallink3?$row.eventkey$</link>
  <link field="msg"> https://externallink4?$row.eventkey$</link>
  <link field="ticket"> https://externallink5?$row.ticket$</link>
</drilldown>
```

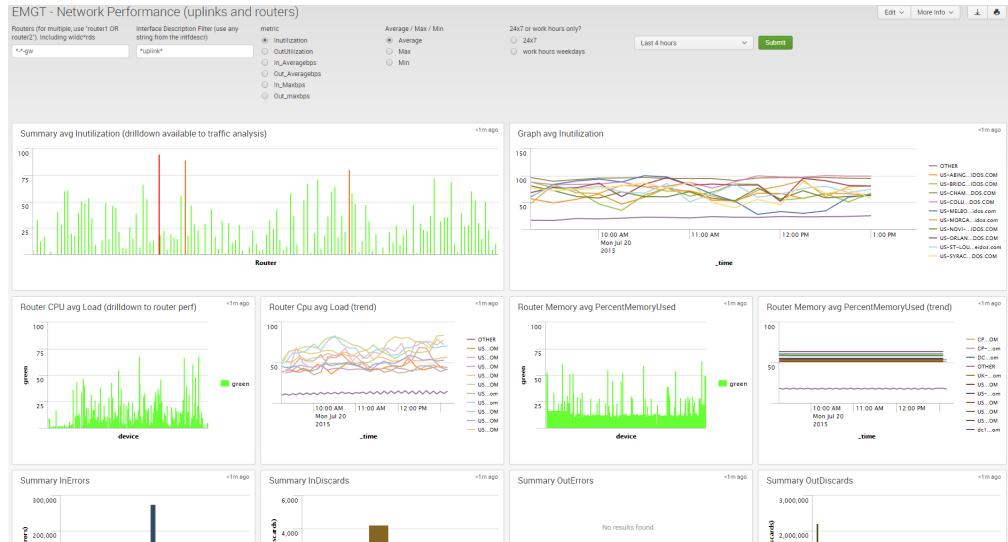
Network: Remote Site Characteristics

- Started with uplink, employees, site support
- Added other network capabilities, has:
 - Firewalls, DHCP appliance, UPS, wireless, etc..
- How:
 - Inputlookup csv
 - Use of multi-selection for mix/match



Network: WAN Performance

- Look at all sites together
- Look at some classic metrics for WAN's
- Use of color to highlight columns
- Drilldown to “*netflow*”, history, others
- *How: DBconnect NPM metric data*



A screenshot of the EMGT interface, showing the search bar highlighted with a red box. The search bar contains the text "*gw" and the interface description filter "*uplink*". Other visible parameters include the metric type (InUtilization), average/max/min selection, and time range (Last 4 hours).

Service Profiling: Lync Servers (KHI)

- Look at all Lync server together
- Color code the metrics
- Drilldown to graphs
- *How:*
 - *Splunk Universal Agent data*
 - *Color via CSV/JS*



ServiceDash - lync - KHIs

host: icp-* metric: Processor % Processor Time Statistic: Avg Show only over threshold: Yes

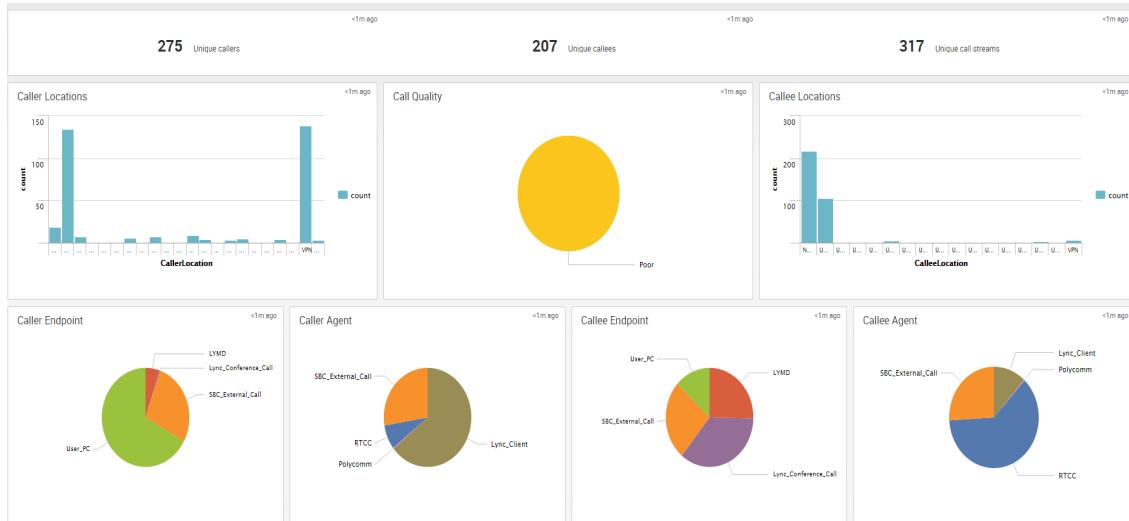
Submit

Service Profiling: Lync Call Quality

- Gather call records
- Report on service metrics and poor quality calls (and from where)

- How:**

- Collect call records via DBconnect*
- Consume CIDR to tie Ipaddresses to locations*



EMGT - Lync call quality

information from the lync mos score records

Search string(s)

Caller Location

Callee Location

Call Quality

Time Period

*

*

*

All

Good Quality

Poor Quality

Last 24 hours

Submit

Explore: Tools for Sysadmins

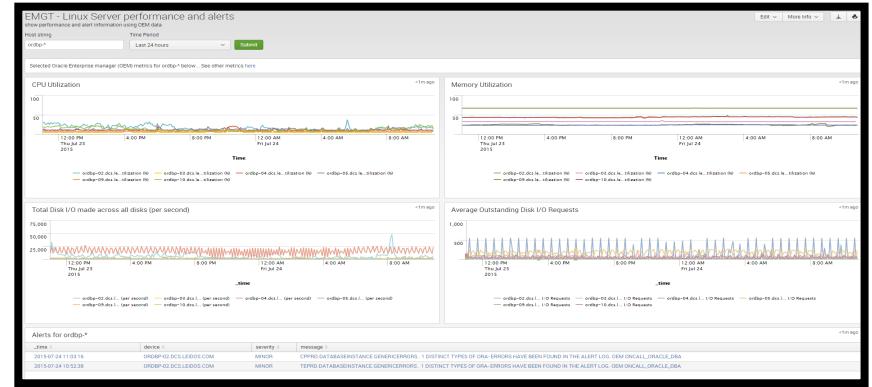
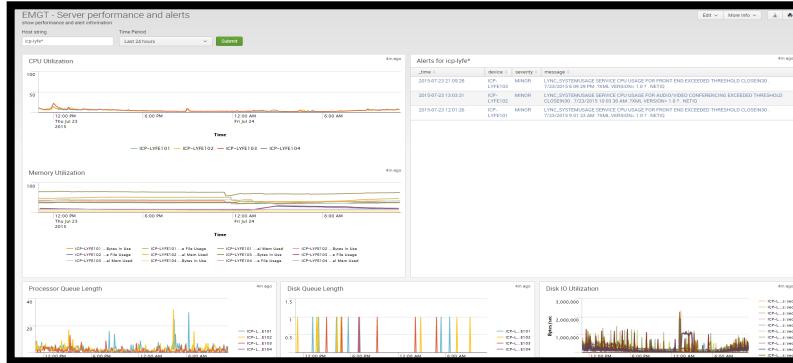
- TopN across 5 key metrics (look across all servers)
- Event logs, reboots, patching

The image displays three Splunk dashboards:

- EMGT - top N servers**: A dashboard showing TopN across five metrics: Cpu, Memory, Processor Queue, Disk Queue, and Disk Space. It includes a search bar for "Host" (set to 25), a time range selector for "When" (Last 60 minutes), and a "Submit" button.
- EMGT - Windows EventLog explorer**: A dashboard for monitoring Windows event logs. It shows a table of events with columns for Date/Time, SourceName, EventCode (EventID), Type, and Message. Below the table are two charts: "Count over time" by SourceName (a line graph) and "By SourceName" (a pie chart).
- EMGT - Windows reboot explorer**: A dashboard for monitoring system reboots. It shows a table of reboots with columns for Date/Time, Server, and Environment (Production, Non-production, QA, Development, Sandbox). Below the table are three charts: "Total Reboots" (a bar chart), "Count by CMDB system" (a bar chart), and "Count by Environment" (a bar chart).

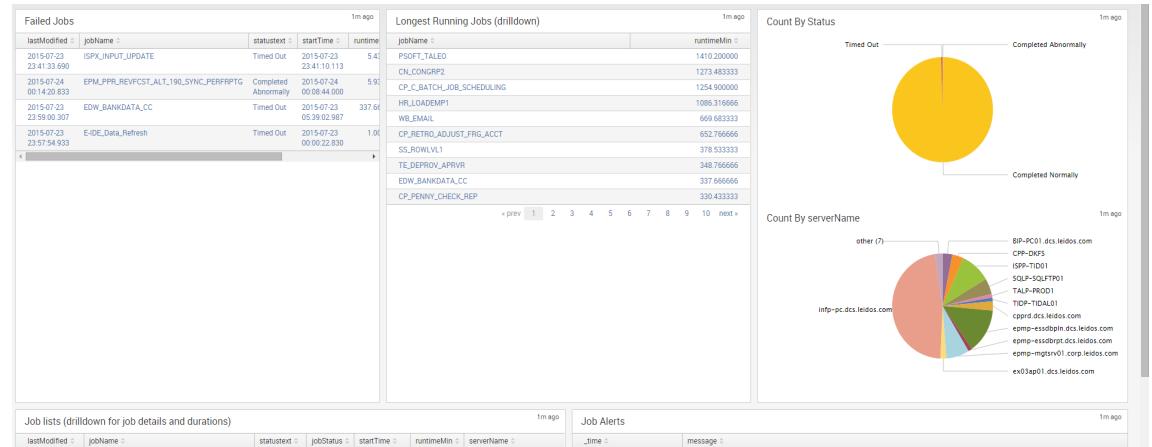
Explore: Server Profiling

- Windows:
 - cpu, memory, process queue, disk stats alerts, reboots, critical eventlogs
 - *How: Splunk universal agent (and some netiq appmanager), alert flow, eventlogs*
- ▶ Linux:
 - cpu, memory, process queue, disk IO
 - *How: DBconnect to Oracle OEM, alert flow*



Explore: Nightly Batch Jobs

- Expose job status to those not using Tidal console
- Use of color to highlight columns
- How:*
 - Dbconnect: Tidal job data*

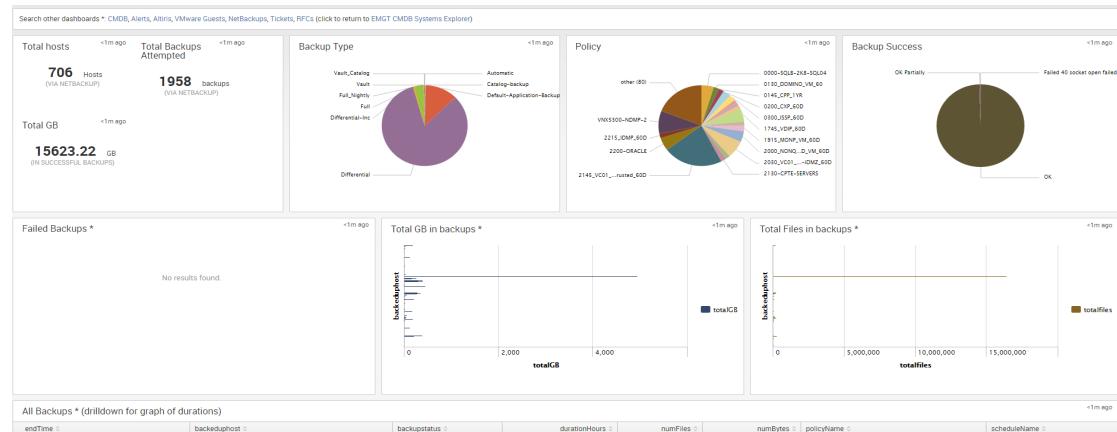


EMGT - Tidal explorer (completed jobs)

JobName	Search String	By server where job ran	Job Status	Time Period	Submit
*	*	*	<input checked="" type="radio"/> All <input type="radio"/> OK only <input type="radio"/> Failed only	Last 24 hours	<input type="button" value="Submit"/>

Explore: Nightly Backups

- Vitally important that backups work
- Service delivery grade for backups defined, as well as working backups
- *How:*
 - *Dbconnect: netbackup/*



Search String (client, policy, schedule)

Backup Type

Duplicates

Exclude dups (SLP*)

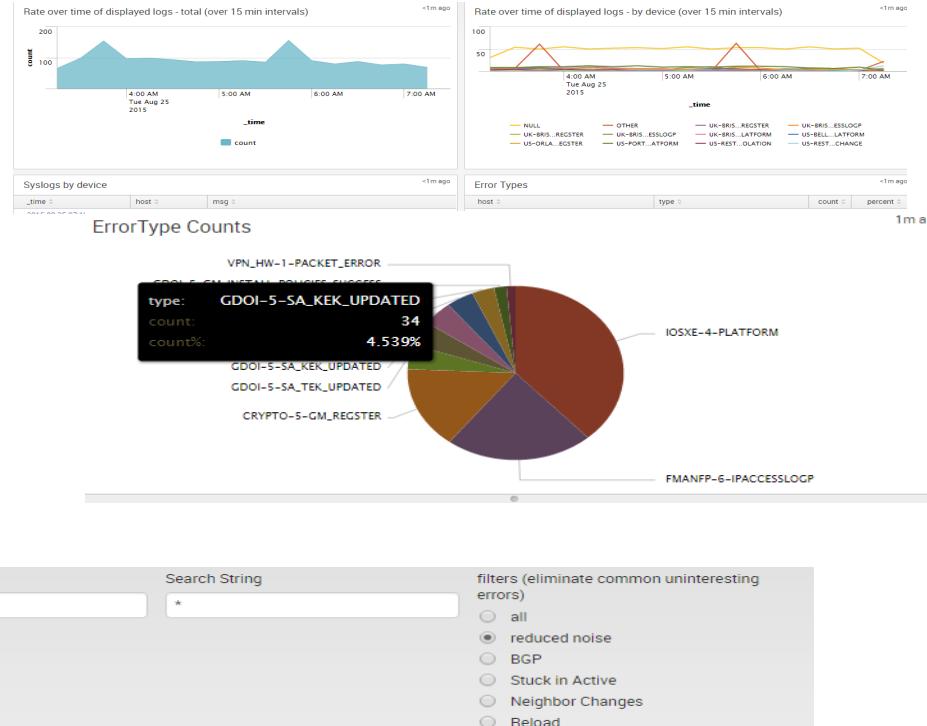
All

Last 24 hours

Submit

Explore: syslogs

- Allow easy inspection and trending of network (and other syslogs)
- Quick searches across device classes (routers, switches, UPS, Vmware, UCS)
- Radio buttons for known situations (BGP flaps, neighbor changes, battery issues)



type <input checked="" type="radio"/> router <input type="radio"/> switch <input type="radio"/> syslog <input type="radio"/> all	DataCenter vs remote <input checked="" type="radio"/> All <input type="radio"/> DataCenter <input type="radio"/> Remote	device *	Search String *	filters (eliminate common uninteresting errors) <input type="radio"/> all <input checked="" type="radio"/> reduced noise <input type="radio"/> BGP <input type="radio"/> Stuck in Active <input type="radio"/> Neighbor Changes <input type="radio"/> Reload
---	---	--------------------	---------------------------	---

Looking Forward

- Consumption of DB/more application logs
- Splunk apps
 - Exchange
 - Active Directory®
 - UCS
 - Clearpass
- Splunk for ITops (“mom”)
- Retirement of EMGTweb v1
- Redouble efforts to get all devices and applications into Splunk
- Better use of data modelling

Status/Performance ▾

ITSM: tickets/changes/onCall ▾

Inventory/CMDB/Grades ▾

Network ▾

Service Dashboards ▾

Explore ▾

Tools ▾

EMGTweb ▾

Dashboards

search

Active Directory is a registered trademarks of Microsoft Corporation in the U.S. and/or other countries.

Thanks

Donald Mahler

ITS Performance Engineering and Systems Monitoring

Email: donald.mahler@leidos.com

Visit us at www.leidos.com



.conf2015

THANK YOU

splunk®



Abstract

- Making Splunk Your Primary IT Information Portal
 - Intermediate | Solutions & Industries: IT Operations, Log Management | Products: Splunk Enterprise | Role: IT Operations Manager, Administrator
- Speakers
 - Donald Mahler, Director Performance management, Leidos
- Over the years, Leidos IT built up a portal for management information; inventory, status, performance, logs, special reports, and more (which was badly in need of a re-design/facelift). Then along came Splunk 6, and we transformed all the critical information displays into a sleek new delivery vehicle. Come and see how.