Little Red Riding CRob and the Big, Scary Log Journey:

aka How I found and fell in love with Splunk

May 19, 2011

Legalese…..

Any views expressed are personal and not necessarily those of KeyCorp.

All examples provided are for illustrative purposes only.

Who Are We?

- Fortune 500 / Top 20 Financial Institution
- Around 19,000 employees
- Over $97 Billion in assets

- Team dedicated to support of mission-critical *NIX-based infrastructure
- Just under 1000 Physical and Virtual servers running 14 different kernel versions across 4 Major OSes
- Piles and Piles of logs sprinkled everywhere

Prologue – Where we use Splunk

All *NIX Syslog messages
*NIX-based Platform Infrastructure and Application logs
Forward security logs from multiple platforms to Enterprise Correlation Engine
Centralized view with Delegated access to application logs

Troubleshooting faster & easier

Comparing/Contrasting servers log volume and results
Find high volume logging servers and pro-actively investigate
***nix app**... provides a global view of performance in comparison against whole environment

Auditing/Alerting/Monitoring

Regulation requirements
“Break The Glass” dashboard – Escalated Access Report

….but we’re getting ahead of ourselves

Once Upon A Time….

Back in days of yore a problem lurked ahead

Manually logged into hundreds of servers

Inconsistent configs & logging

Collected logs and either correlated by hand or used wicked-cool shells scripts to stitch together (lot's of work and prone to "opportunities")

Reactive

Slow

Manual

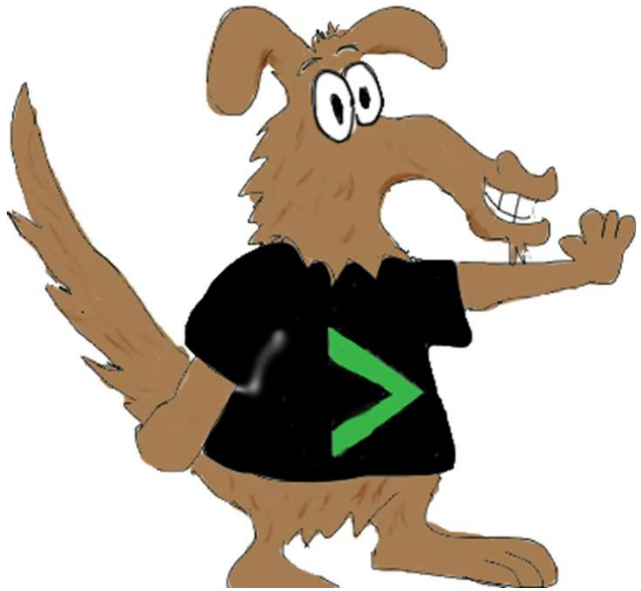
Logs generally ignored until someone made us look or something bad happened

Incomplete picture

How Splunk came to my rescue

NSCD leaky file descriptor and stale thread monitoring
Locked accounts
NAS/SAN connection issues
hardware errors / memory errors
servers acting unstable and logging a lot of things
read-only file systems
Log file delegation instead of LogViewer Websphere app
Server running smoother and cleaner since we get their logs cleaned up
Regulation requirement

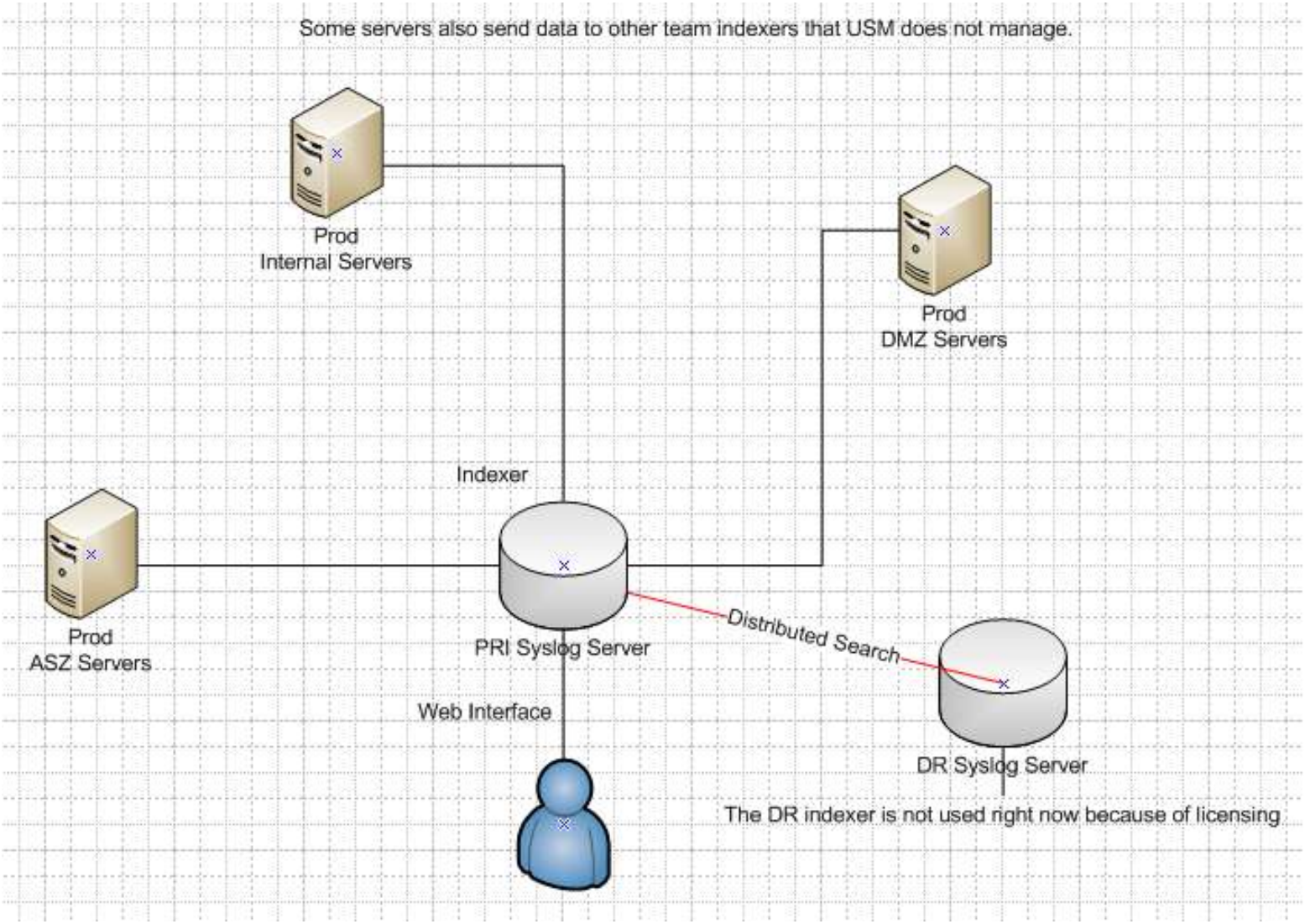
keeping the environment stable and not introducing more downtime



Splunk helped “consume” our logs & use the data

And there was much rejoicing…. yay.

‘Splaining our Splunk



Splunk is deployed to every UNIX-based server.

Some teams also have their own indexers in addition to the Enterprise Splunk.

A Peek into the FUTURE

Client dashboards

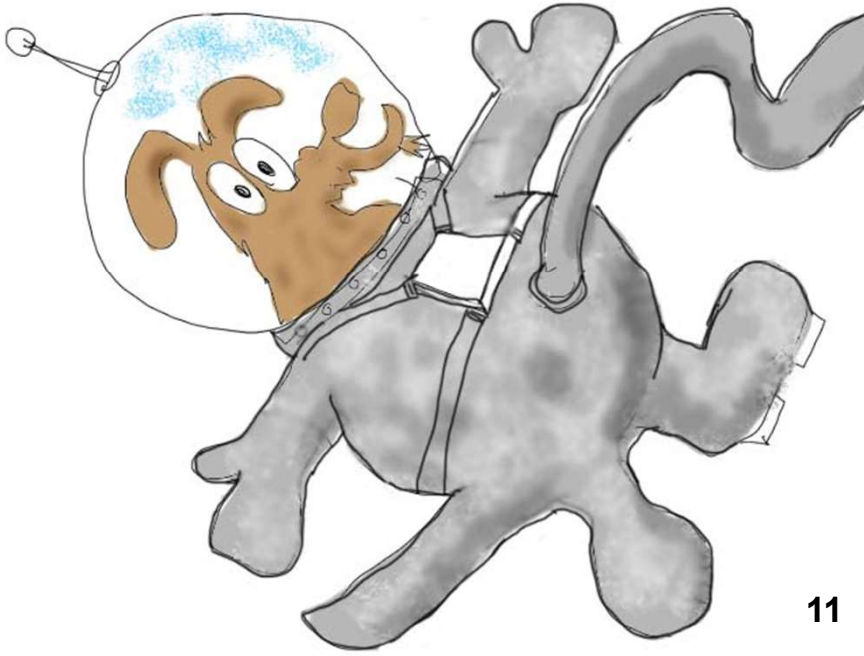
Cross-platform operation log aggregator

Delegated access to logs for development teams

Pci reporting

Performance trending for server consolation

for the peek into the future.. a very important item is really the centralization of being able to query a time and see the os/app/database/web/content engines/etc logs all from a single quick lookup splunkified interface..



It’s not ALWAYS a Happily Ever After….

- AIX
- Dedicated indexers – dedicated headaches (stepping on toes can hurt)
- One Bad Apple… keep an eye on “log spammers” to avoid license blowout

Tips for the Splunk-noob

- **LOOK at your data**.. **understand it**.. /dev/null it if it isn't actionable or important.. Why index and pay for it if its not worth anything? Setup a rotation schedule so that you only keep 6-12months worth of data…once proven get more space later.
- Use restartSplunkd=true in serverclass.conf for deployment server when using scripted install or LWF is in partial config and will spray endlessly same log blowing out license.
- Don't just have splunk monitor a huge directory of files.. cpu usage will be really high and unecessary.. use some regex's.. ie. [monitor:///opt/websphere61] had 127351 files and would chew 50% cpu constantly..
- Even though the LWF will take <1GB.. give it 3GB of space at least to work with. It generates lots of logs internally; tune those down and don't index them unless your going to use them. Internal splunk logs do not count towards licensing
- SupportSSLV3Only = True if you are required to use SSL. Your client browser might require turn off sslv2 or it will be locked out of the GUI.
- Deployment manager as of 4.1.6 can support aix-* which is huge or else you have to define every unique aix server uid. We filed this enhancement request.

Q&A

And they mostly lived happily ever after…….