Getting Started With ELK

SAMSUNG

Ryan MacLean

Senior Engineer
Samsung Research Canada

I'll be your presenter today!

Here's a funny photo of me with a bad moustache, silly haircut and glasses two sizes too large for my face.

I'm a senior engineer for Samsung Research Canada in the B2B Cloud Lab. Look! They even gave me a t-shirt!

These days I spend most of my time on a project called Samsung Pay. This app allows you to pay for things anywhere you can swipe or tap a card for shiny things.

Sort of like this! Samsung Pay isn't available in Canada yet, but we've certainly been working on it!

As you'd expect, this involves a LOT of data, and the ELK stack plays a critical role on a day-to-day basis.

ANSIBLE

GitLab

dynatrace

Java™

python™

NGINX

spring

We use an awful lot of tools at Samsung other than ELK, but here's a NASCAR slide for the ones my team uses the most often.

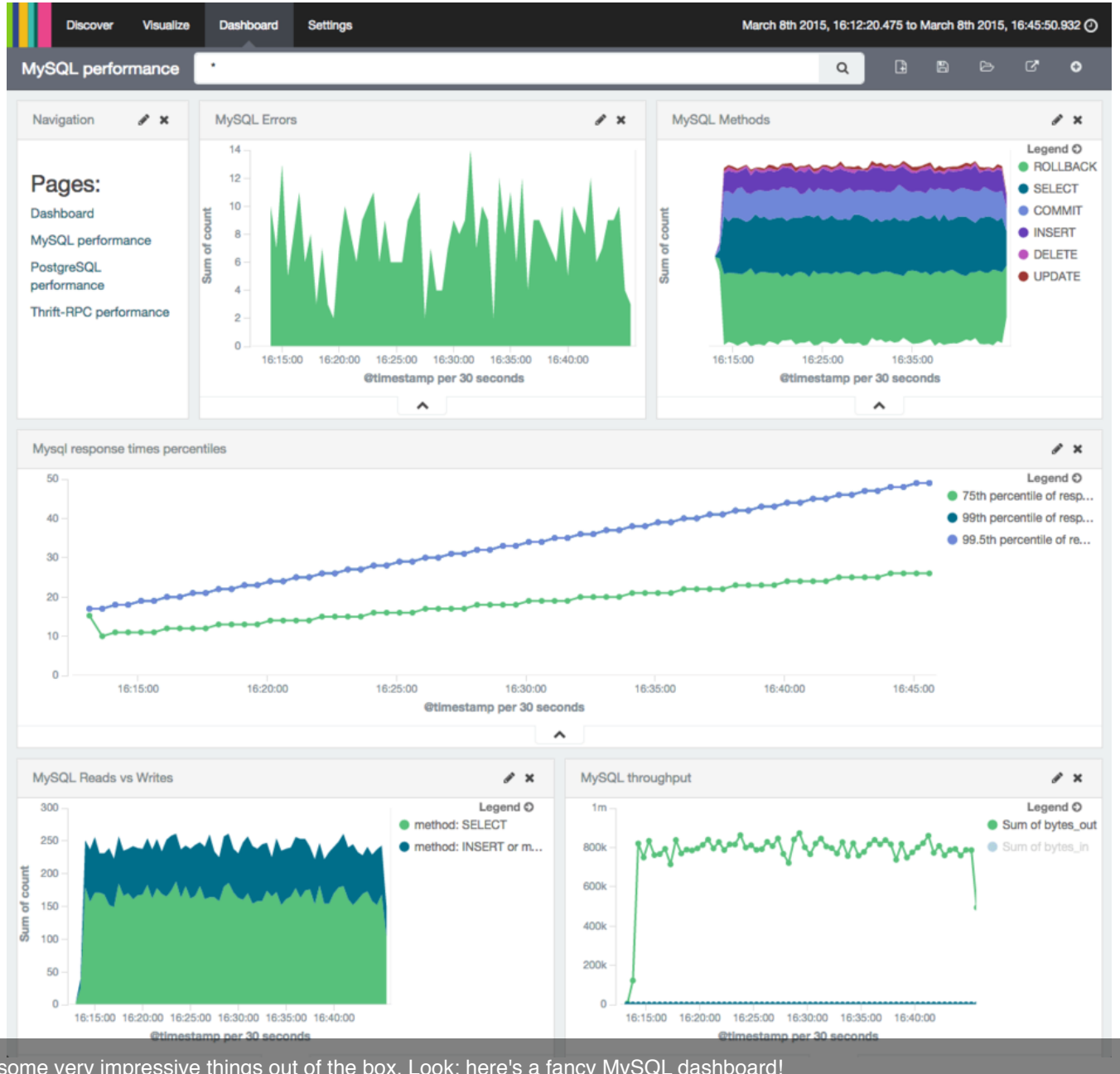
beats

elasticsearch

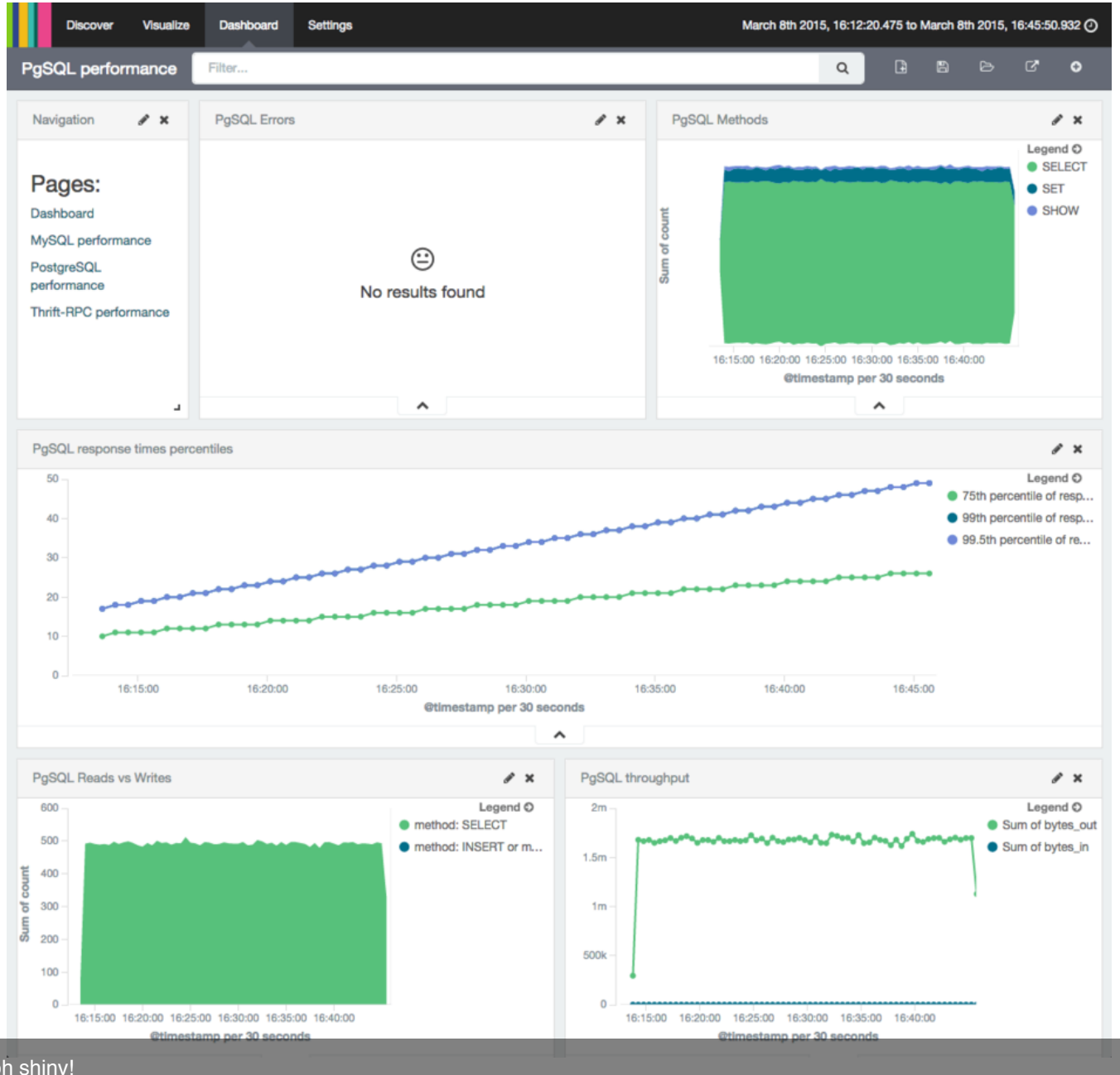
logstash

kibana

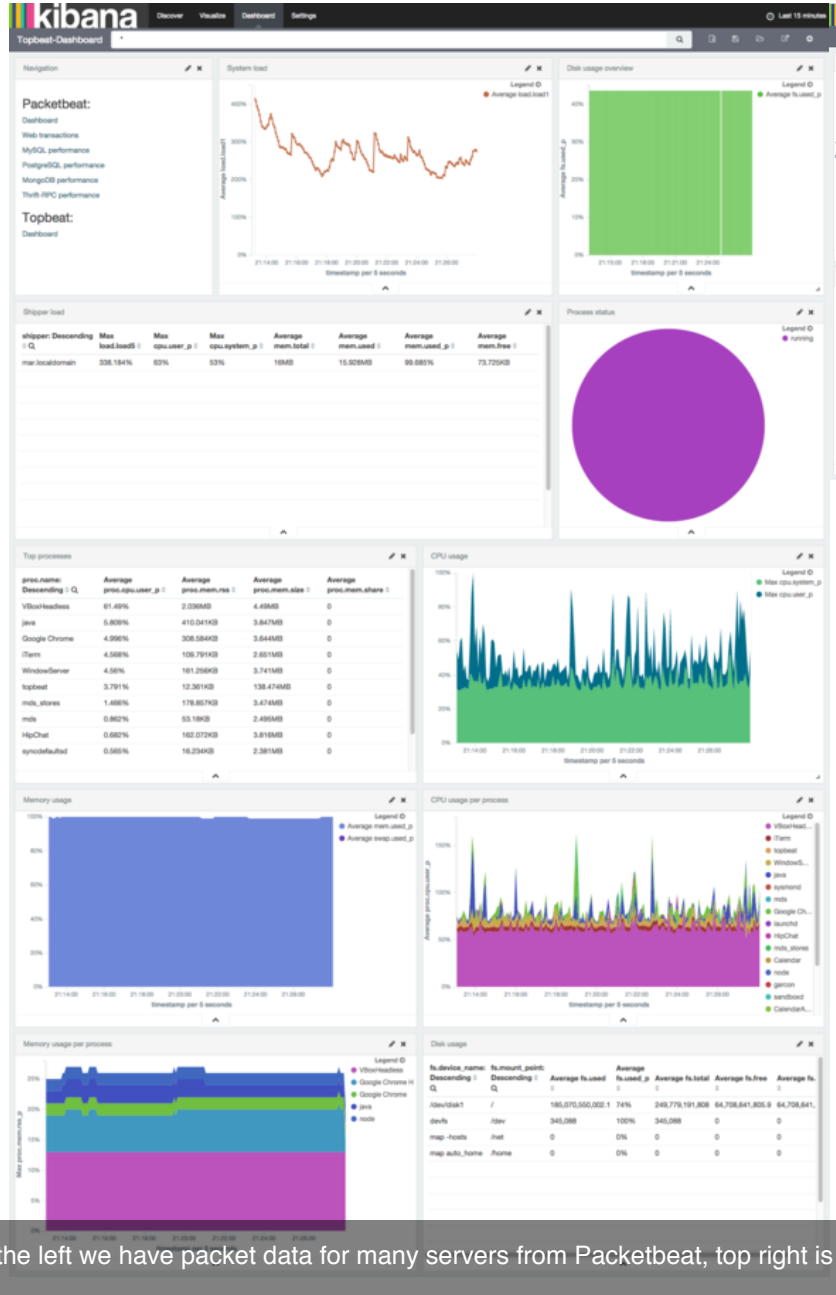
For those of you already using ELK, the only difference between the stack I'm talking about today and the ELK that you are used to is that we're adding Beats. Well Beats and a few other nice things in the background, but mainly Beats.

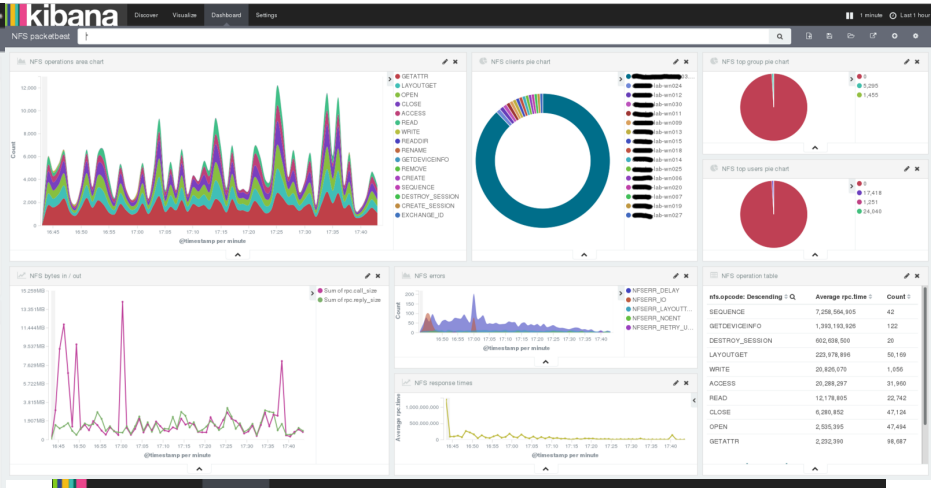


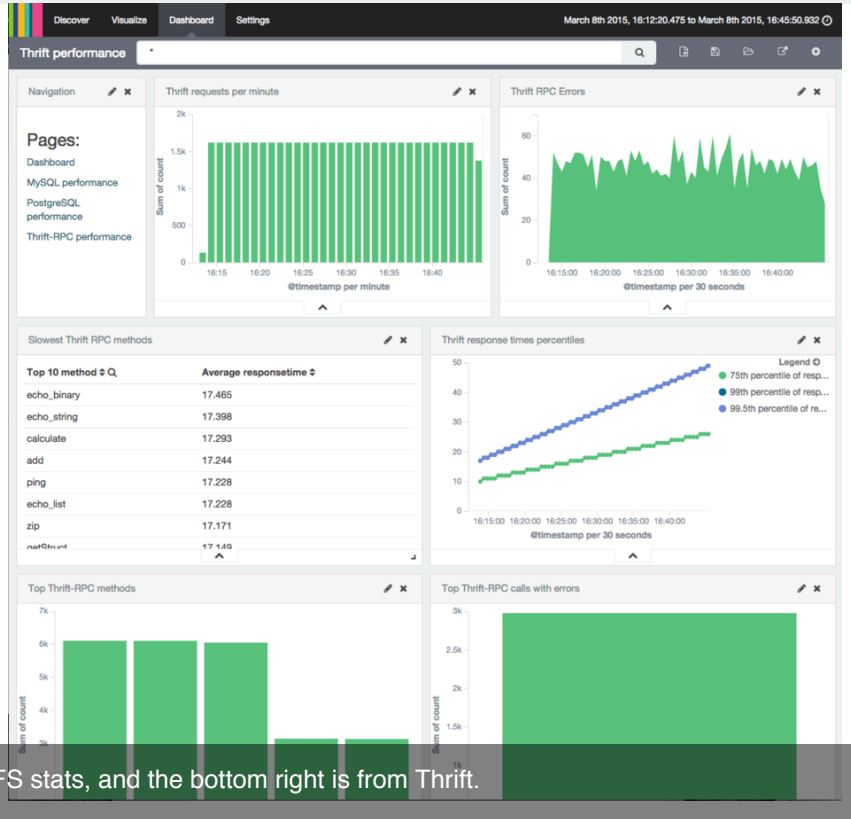
Beats allows us to do some very impressive things out of the box. Look: here's a fancy MySQL dashboard!



And PostgreSQL! Oooh shiny!







On the left we have packet data for many servers from Packetbeat, top right is NFS stats, and the bottom right is from Thrift.

load.sh -url "http://es:9200"

And these are just the default dashboards, one simple command installs them.

First, A Comparison

Let's start off by going over the reasons for building your own ELK stack as you could certainly use Amazon's service, Elastic's offering or third-party tools. Our assumption is that you don't want the data to leave your AWS account, so it leaves us with a couple of free options.

Elastic ElasticSearch VS Your Own

It just rolls off the tongue, right? Elastic Elasticsearch! We'll compare it to a BYOE solution. That's Bring Your Own ElasticSearch for those following along :)

AWS ES

- Fast
- Easy
- 512GB Limit Per Node (10 Node Max)
- Specific Versions
- Limited Plugins
- Limited Vertical Scaling
- Limited Horizontal Scaling

Artisanal ES

- Fast
- Easy-ish
- Limited by Your Wallet
- Mix-and-Match Versions
- Feast on Plugins
- (Virtually) Unlimited Vertical and Horizontal Scaling

* http://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/aes-limits.html

This is a comparison slide. I'm not going to read these bullet points, but rest assured: we're going for the option that allows over 5 terrabytes of storage and more with all the plugins you could think of and dashboards to make any pointy haired boss squeal with delight.

Choose AWS ElasticSearch

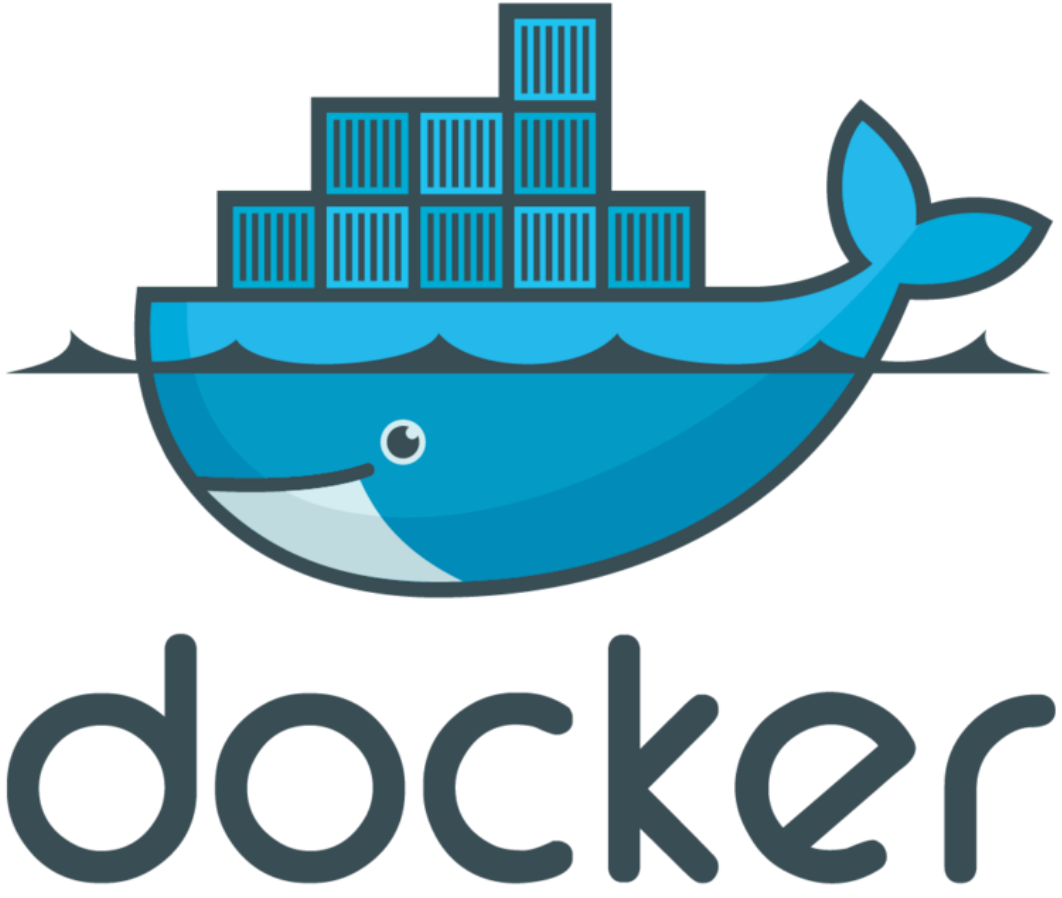
- Only When You're Using AWS
- When You Won't Have More than 512GB for a While
- When You Don't Need Specific Plugins

Just a couple of slides to simplify the decision if ever you're asked about this later.

Choose DIY ElasticSearch

- If You're Not on AWS
- If You Need to Scale Very Quickly
- If Your Measurements Show 512GB Will Not Be Enough

This is of course what we did because we'll be tracking 100s of servers, right?



I tried a lot of different ways to get a script that would make this incredibly quick, and it came down to everyone's favourite buzz-word: Docker. Used with docker-compose, we can link services together and start them with only one command!

GitHub Repository

git pull --recursive https://github.com/ryanmaclean/5-min-elk-stack

First just recursively grab the git repository for this talk.

docker-compose up

It really couldn't be easier!

This assumes you've got both Docker and docker-composed installed, but if not, there are helper scripts for Ubuntu in the tools folder, and links in the readme for Windows, Mac and RPM-based distro users.

Thanks!

DevOps Slack - https://devopschat.co/

Thanks a lot for your time, and if you'd like to chat about this topic or anything else, I can usually be found lurking about in the DevOps Chat Slack.

We're Hiring

The requisite DevOps "we're hiring" slide these days... Please see me after the talk, connect on GitHub or Slack chat or email for more info!