Lecture 35 — DevOps for P4P

Patrick Lam & Jeff Zarnett
patrick.lam@uwaterloo.ca jzarnett@uwaterloo.ca

Department of Electrical and Computer Engineering
University of Waterloo

November 22, 2020

So far, one-off computations: you need to answer a question, so you write code to do that.

But many systems are long-running.
$\Rightarrow$ Operations.

Keep it Rolling

Cloud computing: often long-lived systems, but we didn't talk about how.

Today: many companies fuse development (writes the software) and operations (tends the software).

Disaster Girl Strikes Again

Startups:

No money to pay for separate
developer and operations teams.

Not that many servers,
just a few demo systems, test systems, etc…
but it spirals out from there.

You're not really going to ask Sales to manage these servers, are you?
So, there's DevOps.

DevOps—Good Plan?

Is DevOps a good idea?
Can be used for both good and evil.

Good:

- developers involved across the software lifecycle. (can learn a lot doing ops…)
- developers motivated to use correct tools & document processes.

Configuration as Code

Systems have long come with complicated ("flexible") configuration options.

Sendmail is particularly notorious, but apache and nginx aren't super easy to configure either.

First principle: treat *configuration as code*.

Configuration as Code

- use version control on your configuration.
- implement code reviews on changes to the configuration.
- test your configurations.
- aim for a suite of modular services that integrate together smoothly.
- refactor configuration files.
- use continuous builds (more on that later).

Autoconfig

Excellent idea: tools for configuration.

Not enough to write text
"How to Install AwesomeApp"

e.g. use Terraform—
build, installation, and update automatic & simple.

Complicated means mistakes. . . people forget steps.
They are human.

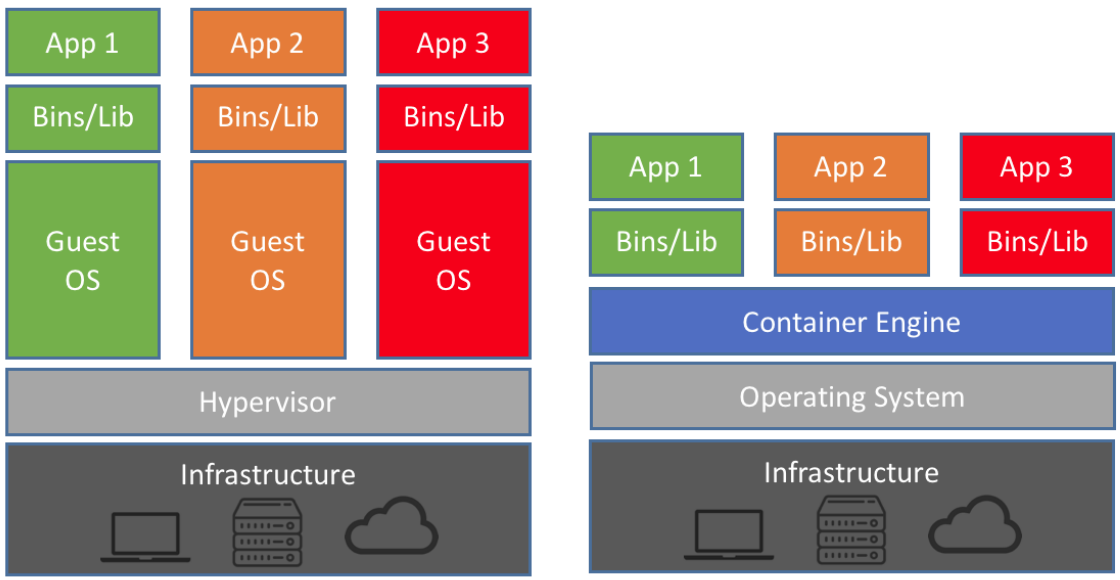
Its whole purpose is to manage your config as codes situation where you want to run your code using a cloud provider (e.g., AWS),

Containerize Me, Captain

How Did We Get Here?

- Manual install
- Package Manager (RPM/JAR/DLL Hell)
- Virtual Machines
- Containerization

See this diagram from NetApp:



Security, Report to the Bridge

Having an always-available service accessible over the internet makes security a very big concern.

Risk Enormous

You can run some program with tons of security vulnerabilities offline and feel that the security problems can be managed.

When it's online the risk is enormous.

All kinds of vulnerabilities are a problem, but I'll call out two of them:

Code execution/injection and data leakage (information exposure).

GDPR Says What

https://enforcementtracker.com/

Audit This

There are some companies out there that will check your code for libraries with versions having known security vulnerabilities.

Sadly, when there is an updated version of a library, there may be breaking changes in it...

Checking for vulnerabilities should be an automatic process as part of your build and release procedures.

Servers as Cattle, not Pets

Servers means servers, or virtual machines, or containers.

At scale (smaller than you think):
use mass tools for dealing with servers,
rather than doing tasks manually.

At least: cloud-like server initialization without manual intervention;
must be able to spin up a server programmatically.

Another Example

This is used to automate deploying and scaling of applications.

Common Infrastructure

Use APIs to access your infrastructure. Examples:

- storage
- naming and discovery
- monitoring

Avoid one-offs—use open-source tools when applicable.
But build your own tools if needed.

Oh, Think Twice...

Is this what we are best at?

Think extra carefully if you plan to do roll your own anything that is security or encryption related.

A breach of data protection regulations can get very expensive. See `https://www.enforcementtracker.com/`

Rule of Ten

eBay:

- 1995: perl scripts;
- 1997: C++/Windows;
- 2002: Java.

Each of these architectures was appropriate at the time, but not as requirements changed.

More sophisticated successor architectures would have been overkill earlier.

Hard to predict what's needed in the future.

Naming

Naming is one of the hard problems in computing.

There are only two hard things in computers:

1. cache invalidation,
2. naming things, and
3. off by one errors.

Naming Suggestions

- use canonical one-word names for servers;
- but, use aliases to specify functions, e.g. 1) geography (nyc); 2) environment (dev/tst/stg/prod); 3) purpose (app/sql/etc); and 4) serial number.

There's also the Java package approach of infinite dots: live.application.customer.webdomain.com or however you want to call it.

Pick something and be consistent.

Continuous Integration

- pull code from version control;
- build;
- run tests;
- report results.

Continuous Integration Social Convention

Don’t break the build (or donuts).

Run the CI cycle on every commit;
results sent by e-mail or instant messenger.

Canarying

Canarying

Deploy new code incrementally in production, also known as “test in prod”:

- stage for deployment;
- remove canary servers from service;
- upgrade canary servers;
- run automatic tests on upgraded canaries;
- reintroduce canary servers into service;
- see how it goes!

Of course: implement your system with rollback.

Monitoring

Things to think about:

- CPU Load
- Memory Utilization
- Disk Space
- Disk I/O
- Network Traffic
- Clock Skew
- Application Response Times

Dashboard

Multiple systems: need an overview of all the systems.

Summary needs to show whether anything is wrong,
but not an overwhelming wall of data.


ALERT
CONDITION: RED

Dashboard

Don’t pay someone to stare at the dashboard and
press the “Red Alert!” button
if anything goes out of some preset range.

No, for that we need some automatic monitoring.

Red Alert

- **Alerts**: a human must take action now;
- **Tickets**: a human must take action soon
  (hours or days);
- **Logging**: no need to look at this
  except for forensic/diagnostic purposes.

Common bad situation: logs-as-tickets.


Feuerwehr
Scheibe einschlagen
Knopf tief drücken

Action Stations! Set Condition One Throughout the Ship

What do you do when you hear the fire alarm?

If there is an actual fire, you will not only be wrong, you might also be dead.

Not the Kittens!!!

Alerts and tickets are a great way to make user pain into developer pain.

Some SUPER CRITICAL ticket OMG KITTENS ARE ENDANGERED is an excellent way to learn the lesson...

Devs will take steps that keep these things from happening in the future.