
@axelfontaine
IMMUTABLE
INFRASTRUCTURE
RISE OF THE MACHINE IMAGES

About Axel Fontaine

- Founder and CEO of Boxfuse
- Over 15 years industry experience
- Continuous Delivery expert
- Regular speaker at tech conferences
- JavaOne RockStar

@axelfontaine

boxfuse

flywaydb.org

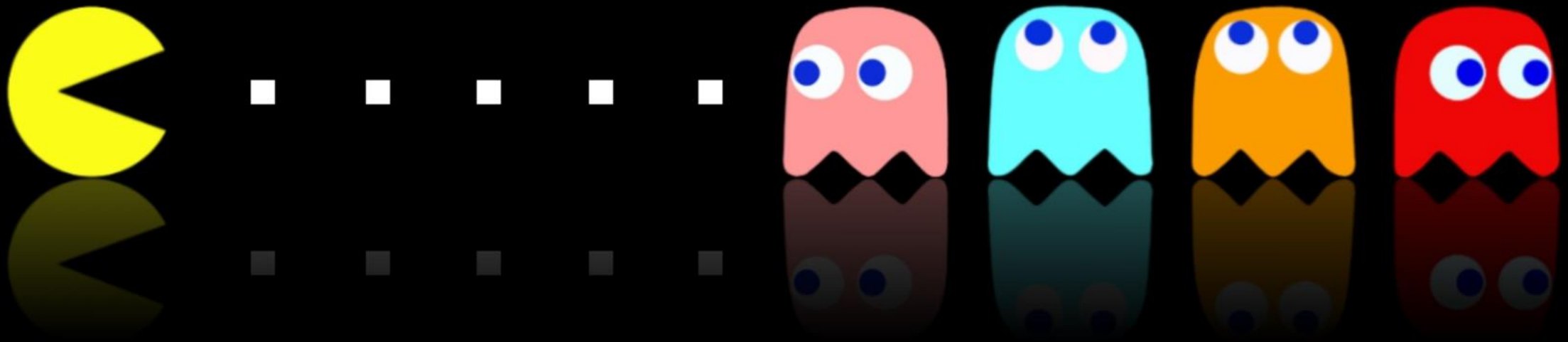
boxfuse

boxfuse.com

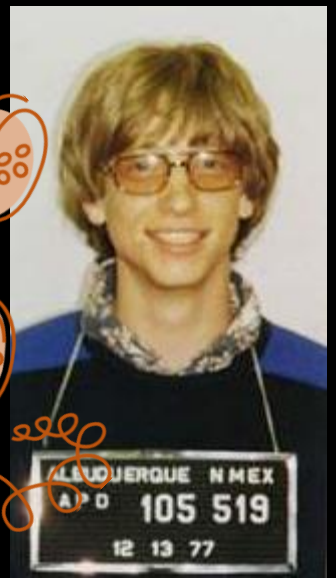
about

questions

sometime in the 20th century …



http://en.wikipedia.org/wiki/File:Tdkc60cassette.jpg


ALBUQUERQUE N MEX
105 519
12 13 77


Microsoft
Windows NT
Server

Challenges

ON PREM =

+

+

- ✓ OS Install
- ✓ OS Patching
- ✓ App Install
- ✓ App Updates

- ✓ Procurement
- ✓ Vendor Mgmt
- ✓ Capacity Plan.
- ✓ Financing

- ✓ Power
- ✓ Network
- ✓ Cooling
- ✓ Phys. Security
- ✓ Phys. Space

boxfuse

Challenges

ON PREM =

+

- ✓ OS In
- ✓
- ✓ Capacity Plan.
- ✓ Financing

- ✓ Power
- ✓ Network
- ✓ Cooling
- ✓ Phys. Security
- ✓ Phys. Space

Lots of undifferentiated heavy lifting


FNB
GOLD Credit Card
4000 1234 5678 9010
4127
EXPIRES END 05/84
SARAH CONNOR
VISA

Challenges

ON PREM =

+

+

- ✓ OS Install
- ✓ OS Patching
- ✓ App Install
- ✓ App Updates

- ✓ Procurement
- ✓ Vendor Mgmt
- ✓ Capacity Plan.
- ✓ Financing

- ✓ Power
- ✓ Network
- ✓ Cooling
- ✓ Phys. Security
- ✓ Phys. Space

🕘 Hours

🕘 Days or Weeks

🕘 Months

boxfuse

Challenges

COLO = 

+  **+** 

- ✓ OS Install
- ✓ OS Patching
- ✓ App Install
- ✓ App Updates

🕘 Hours

- ✓ Procurement
- ✓ Vendor Mgmt
- ✓ Capacity Plan.
- ✓ Financing

🕘 Days or Weeks

- ✓ Power
- ✓ Network
- ✓ Cooling
- ✓ Phys. Security
- ✓ Phys. Space

🕘 Months

boxfuse

Challenges

ROOT SERVER =

+

+

- ✓ OS Install
- ✓ OS Patching
- ✓ App Install
- ✓ App Updates

- ✓ Procurement
- ✓ Vendor Mgmt
- ✓ Capacity Plan.
- ✓ Financing

- Hours
- Days or Weeks

boxfuse

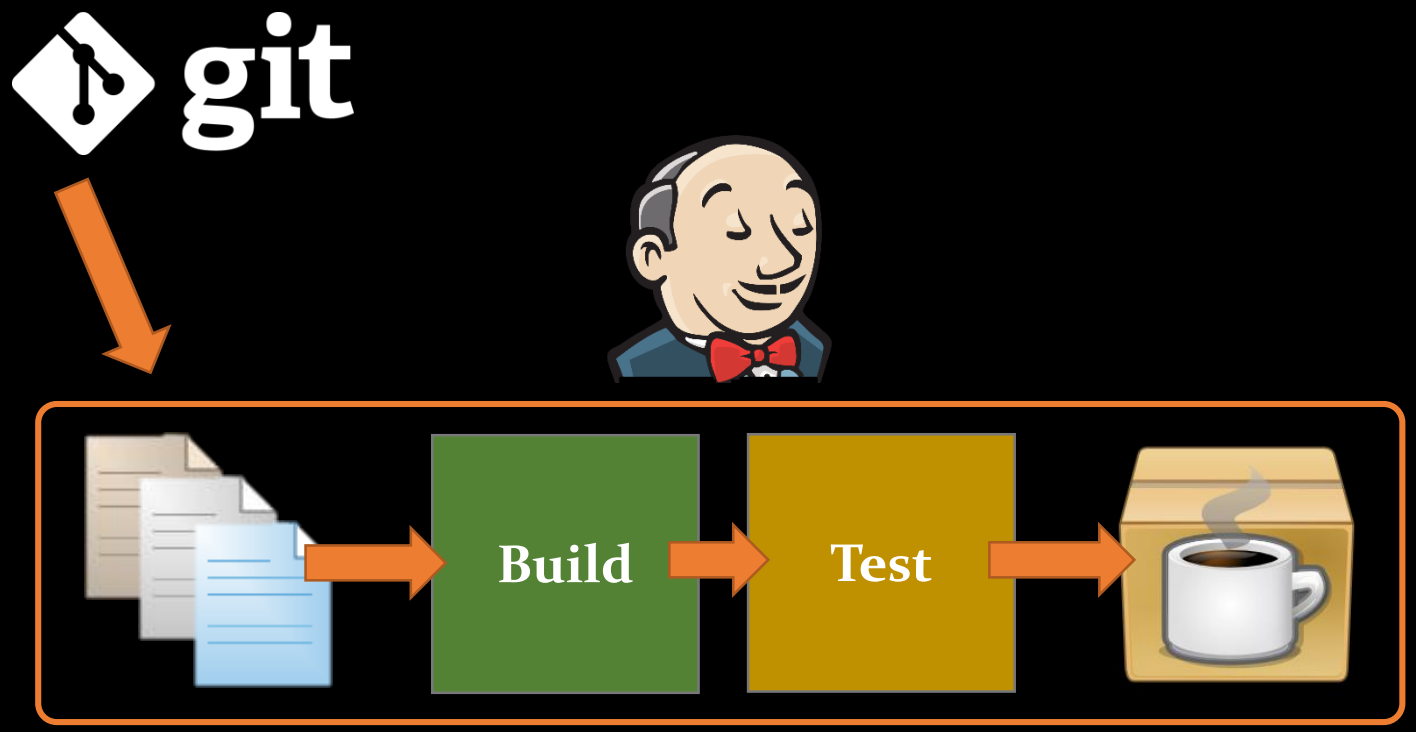
Let’s talk about software

- ✓ OS Install
- ✓ OS Patching
- ✓ App Install
- ✓ App Updates

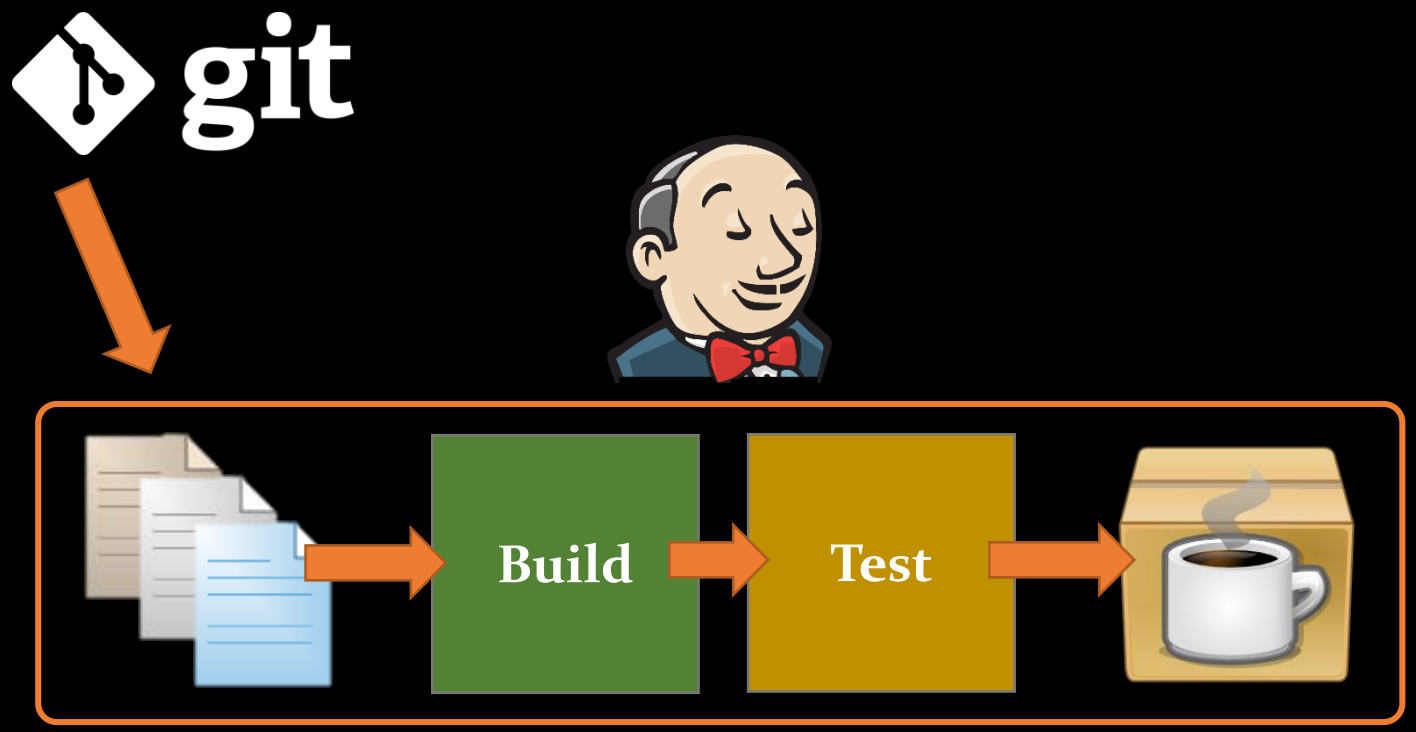
boxfuse

POLL:
which level of automation are you at?

- ✓ Build
- ✓ Unit Tests
- ✓ Continuous Integration
- ✓ Acceptance Tests
- ✓ Continuous Deployment (Code)
- ✓ Continuous Deployment (Code + DB + Configuration)
- ✓ Infrastructure



boxfuse



boxfuse

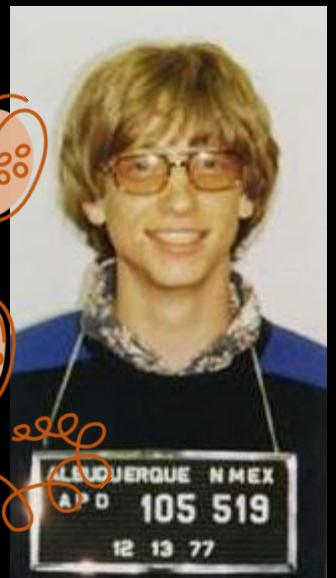
- One immutable unit
- Regenerated after every change
- Promoted from Environment to Environment

Classic Mistake: Build per Environment

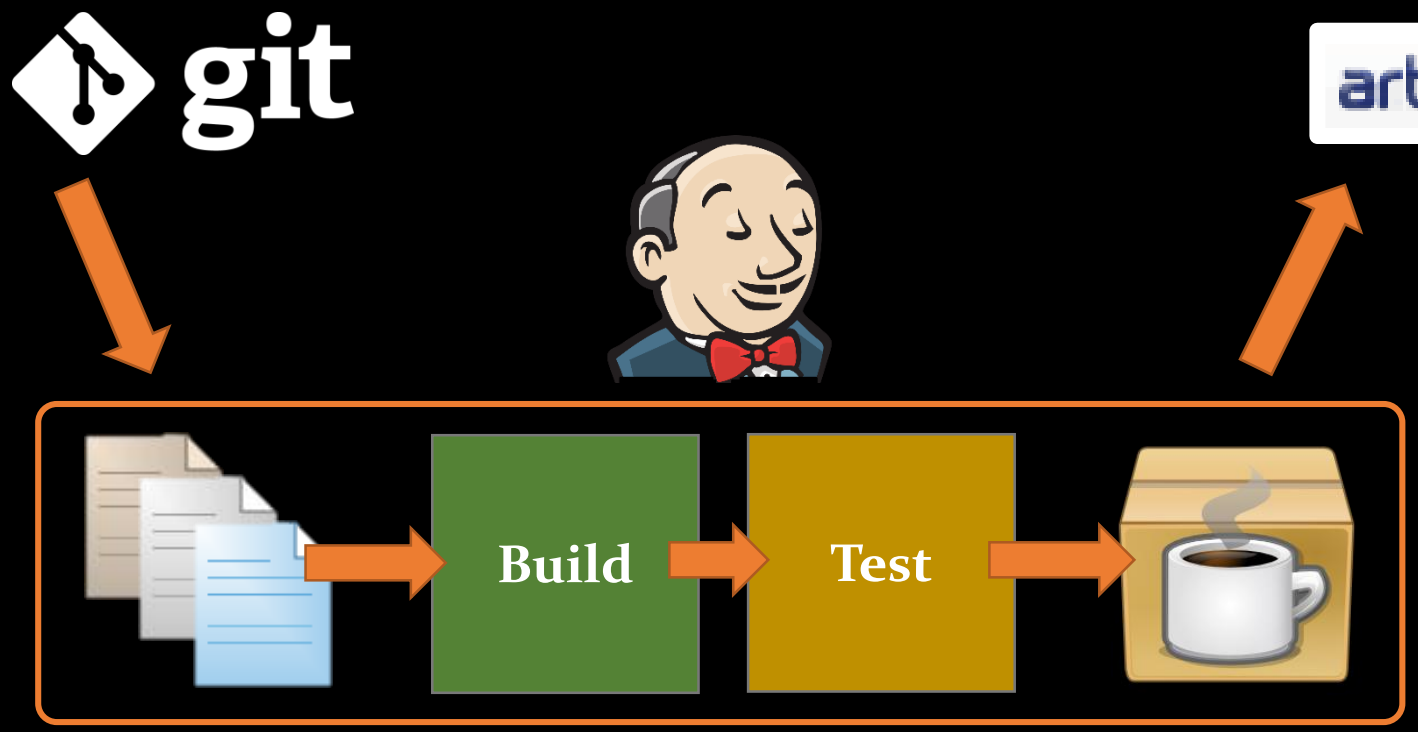
boxfuse

boxfuse

why aren’t we doing the same
for the layers this is running on ???

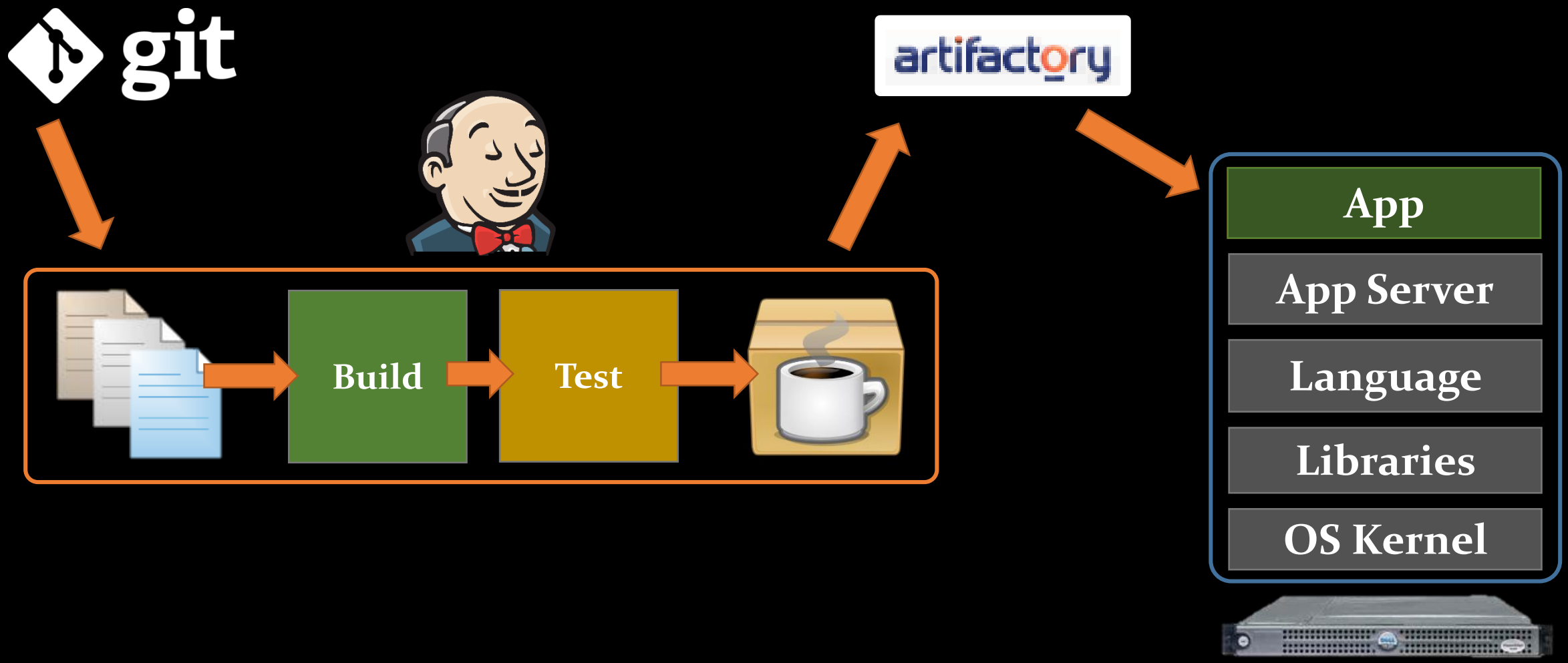

ALBUQUERQUE N MEX
105 519
12 13 77


Microsoft
Windows NT
Server

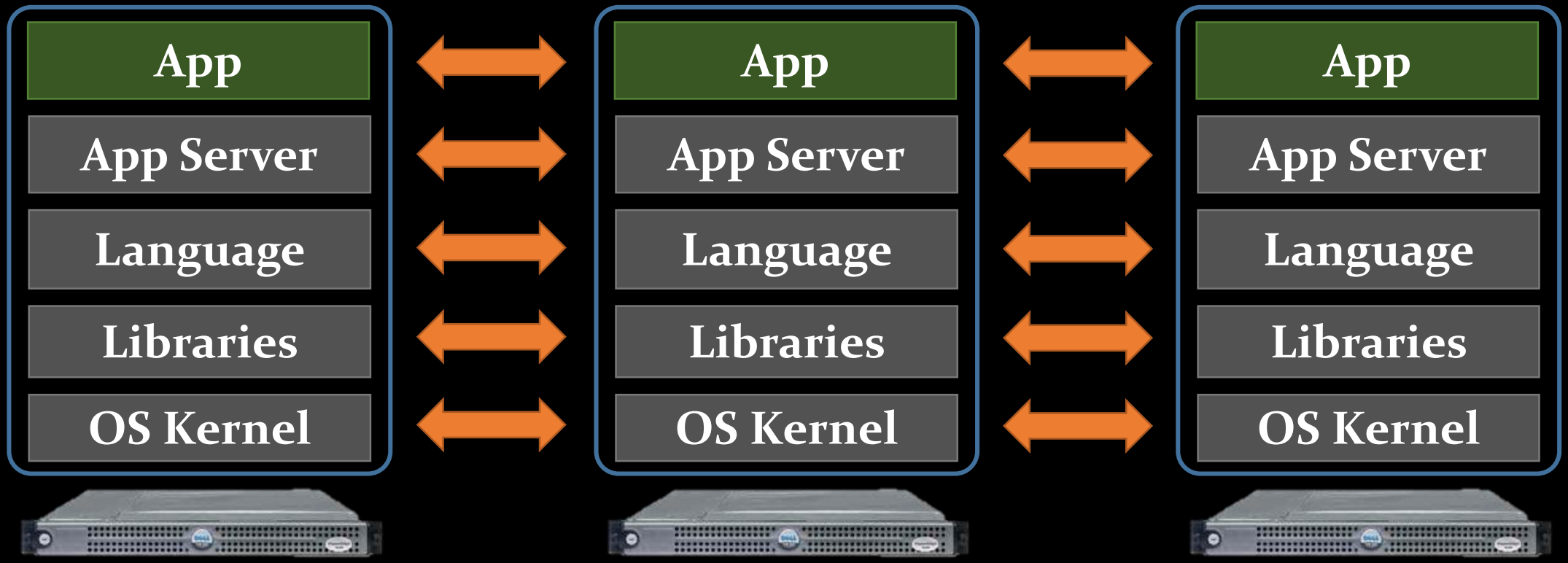

git
artifactory
Build
Test


App
App Server
Language
Libraries
OS Kernel

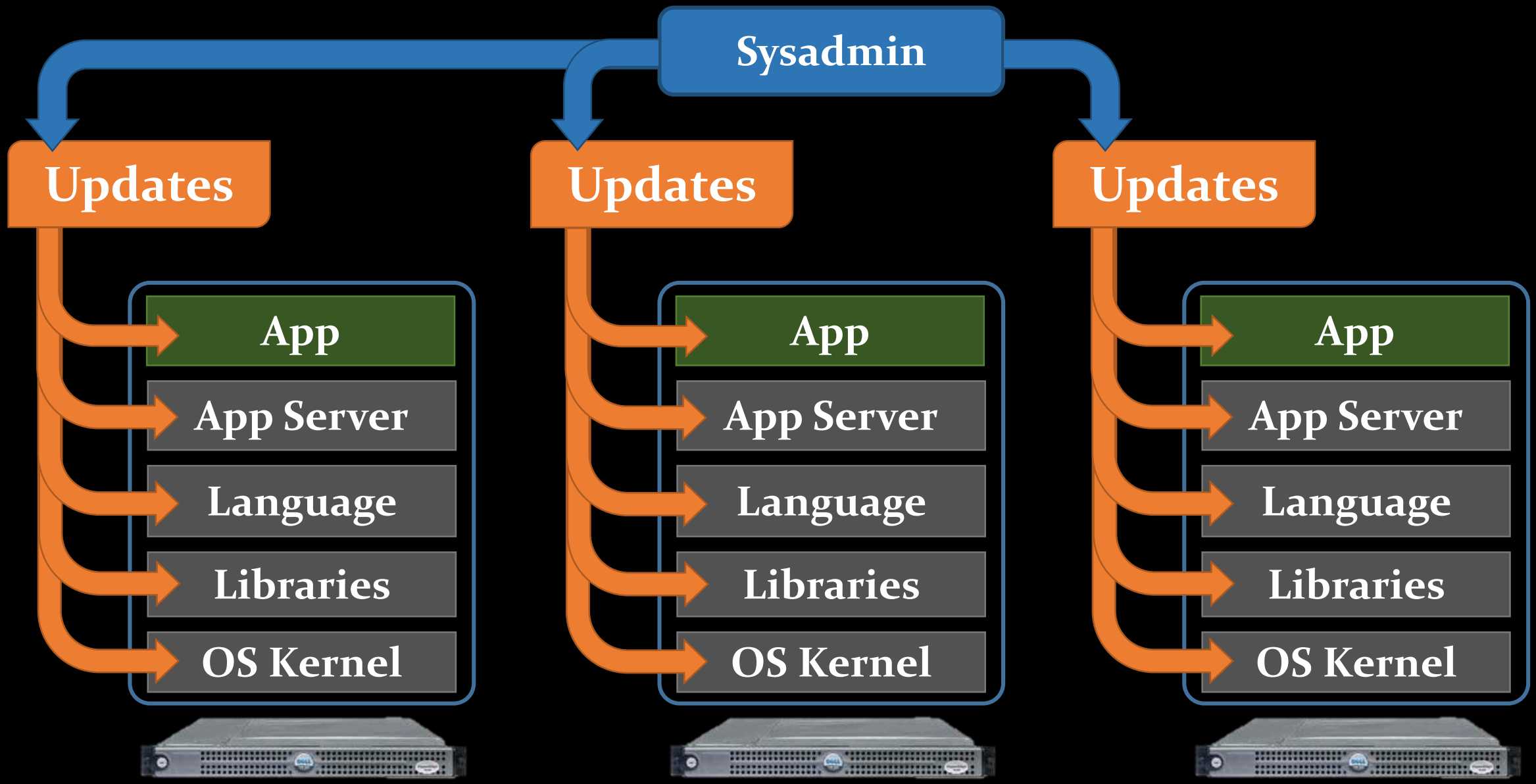
boxfuse


git
artifactory
Build
Test
App
App Server
Language
Libraries
OS Kernel

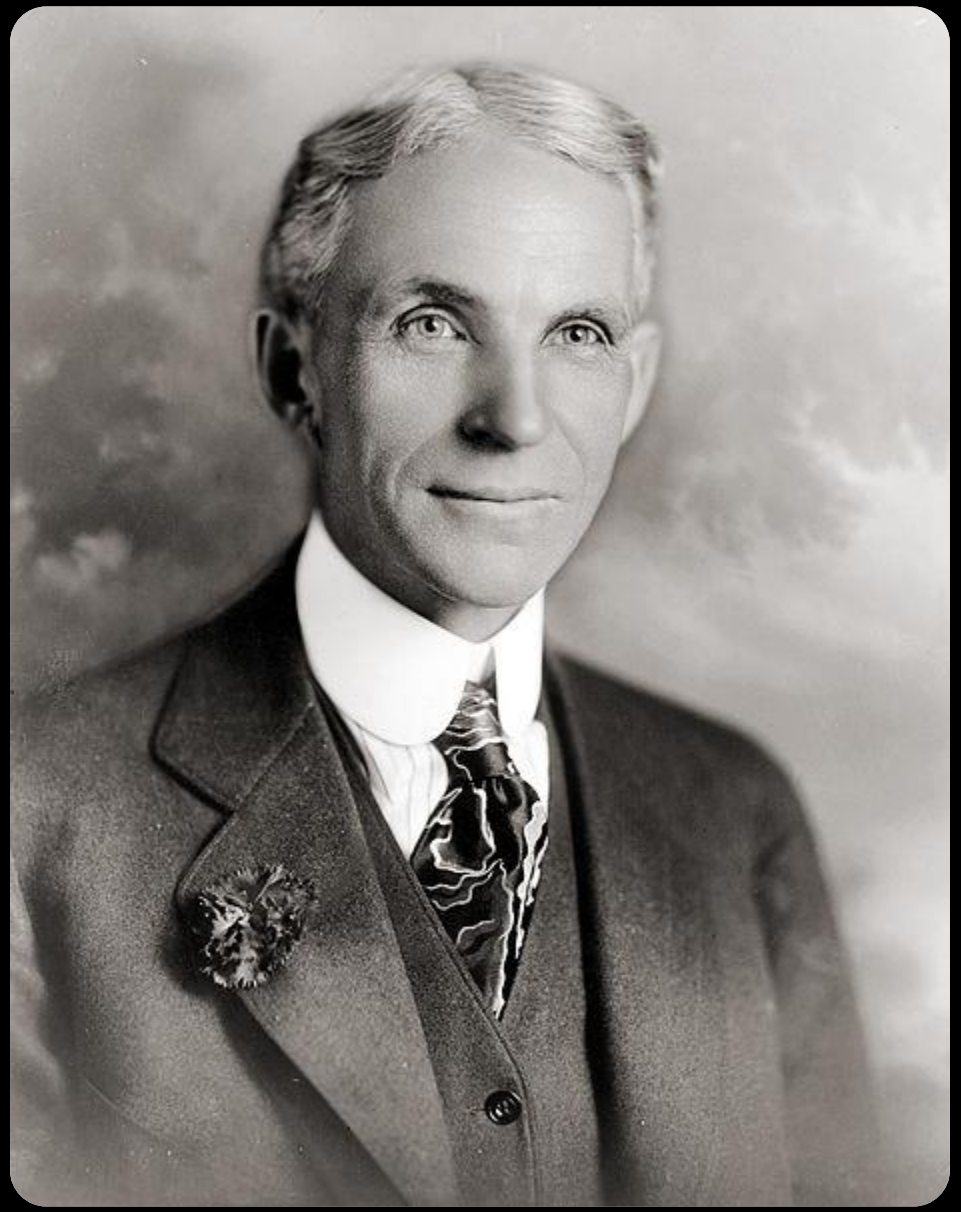
Any difference is a potential source of errors



boxfuse


Sysadmin
Updates
Updates
Updates
App
App Server
Language
Libraries
OS Kernel
App
App Server
Language
Libraries
OS Kernel
App
App Server
Language
Libraries
OS Kernel

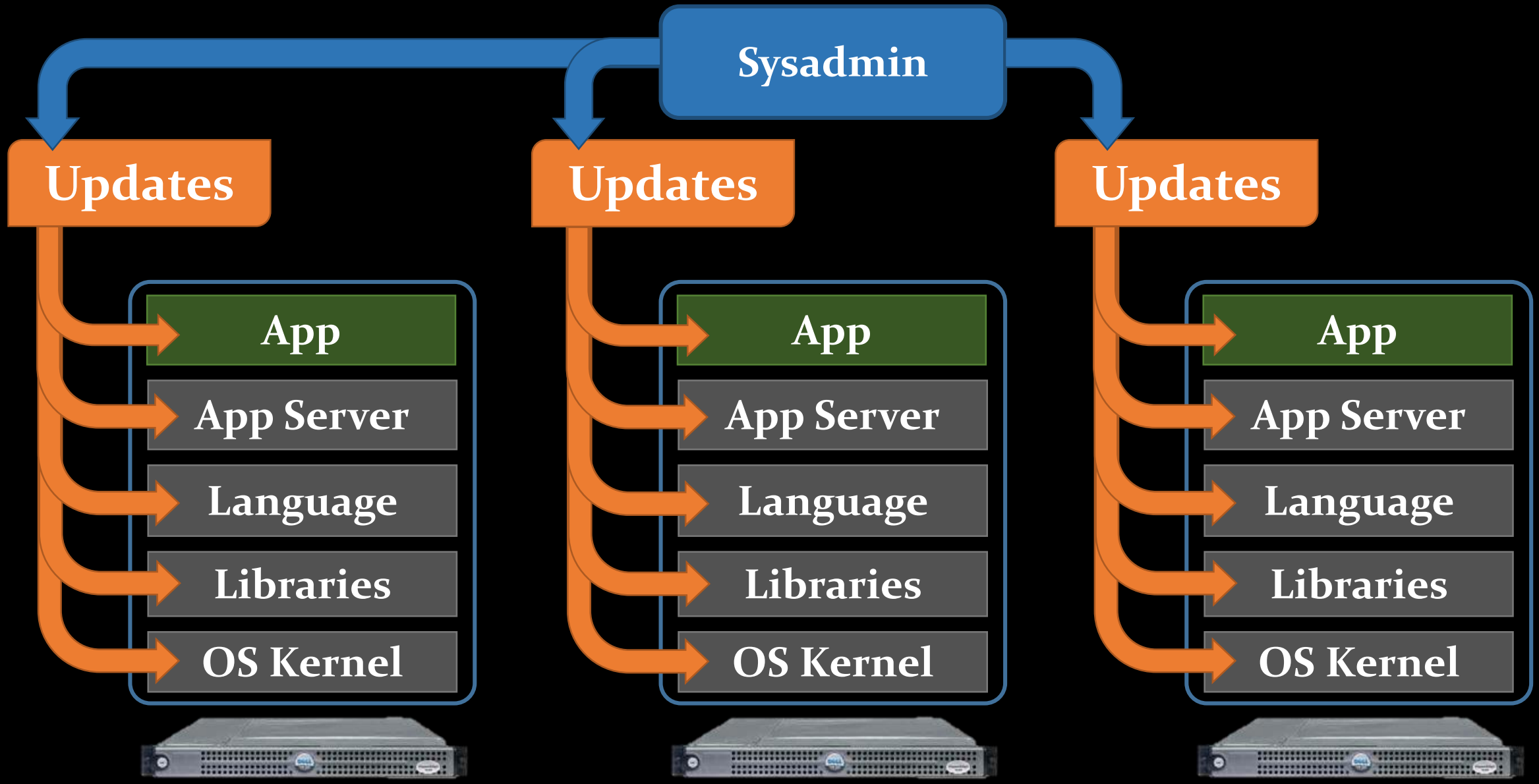
boxfuse



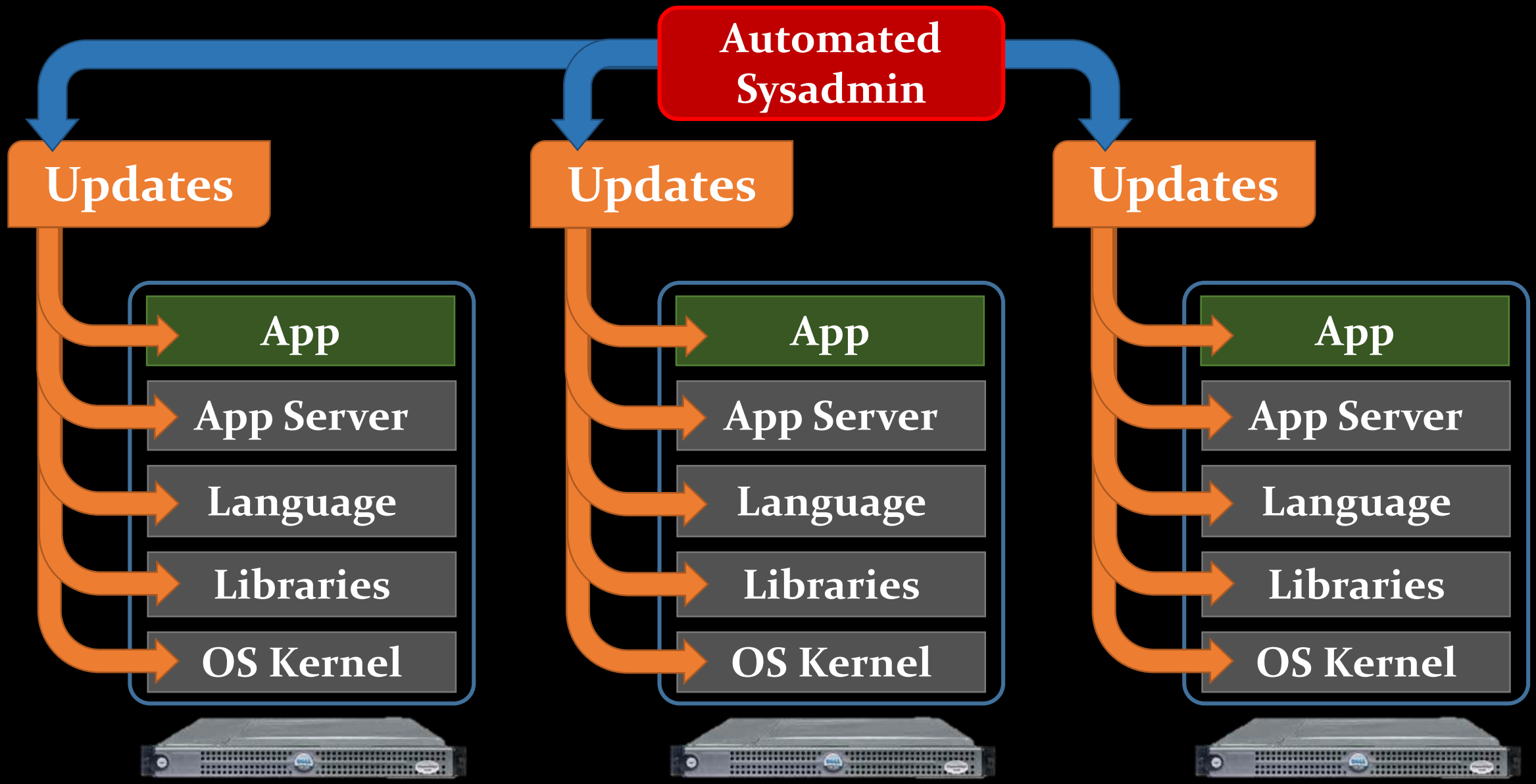
If I had asked my customers what they wanted they would have said a faster horse.

Henry Ford

boxfuse


Sysadmin
Updates
Updates
Updates
App
App Server
Language
Libraries
OS Kernel
App
App Server
Language
Libraries
OS Kernel
App
App Server
Language
Libraries
OS Kernel

boxfuse


Automated Sysadmin
Updates
Updates
Updates
App
App Server
Language
Libraries
OS Kernel
App
App Server
Language
Libraries
OS Kernel
App
App Server
Language
Libraries
OS Kernel

boxfuse

fast forward to 2016 …

Every day, AWS adds enough server capacity to power the whole $7B enterprise Amazon.com was in 2004.
Weekends included.

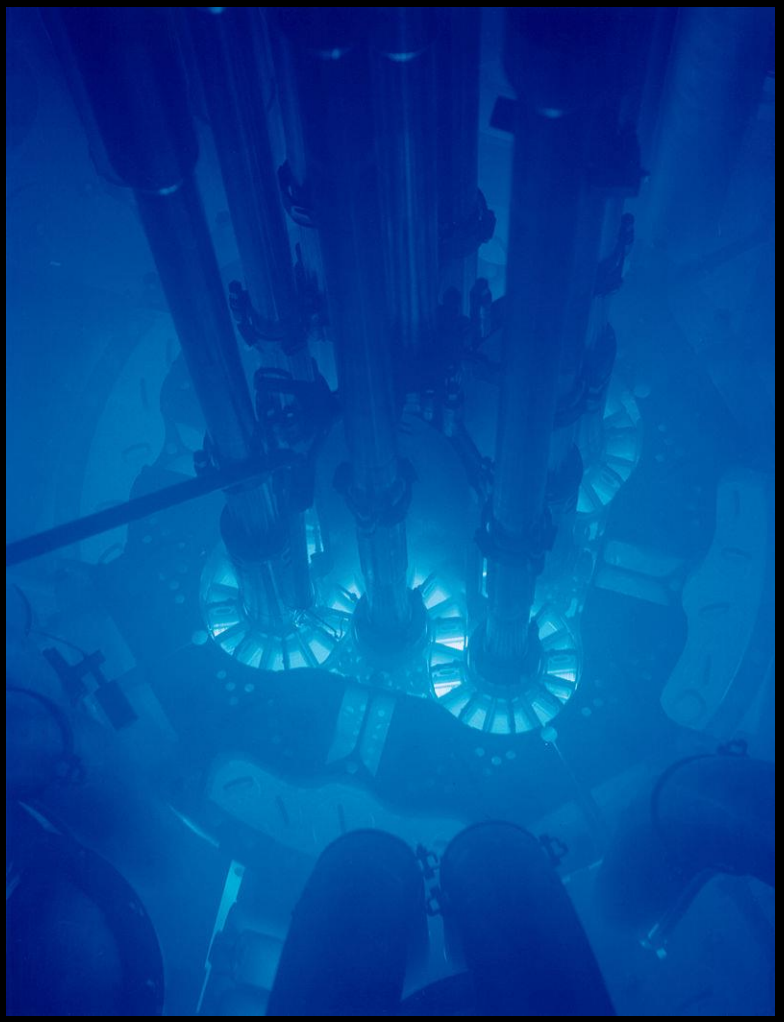
amazon web services

boxfuse

Shift to a world of abundance
(no more resource scarcity)

"RIAN archive 341194 Kursk Nuclear Power Plant" by RIA Novosti archive, image #341194 / Sergey Yakimov / CC BY-SA 3.0. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:RIAN_archive_341194_Kursk_Nuclear_Power_Plant.jpg#mediaviewer/File:RIAN_archive_341194_Kursk_Nuclear_Power_Plant.jpg

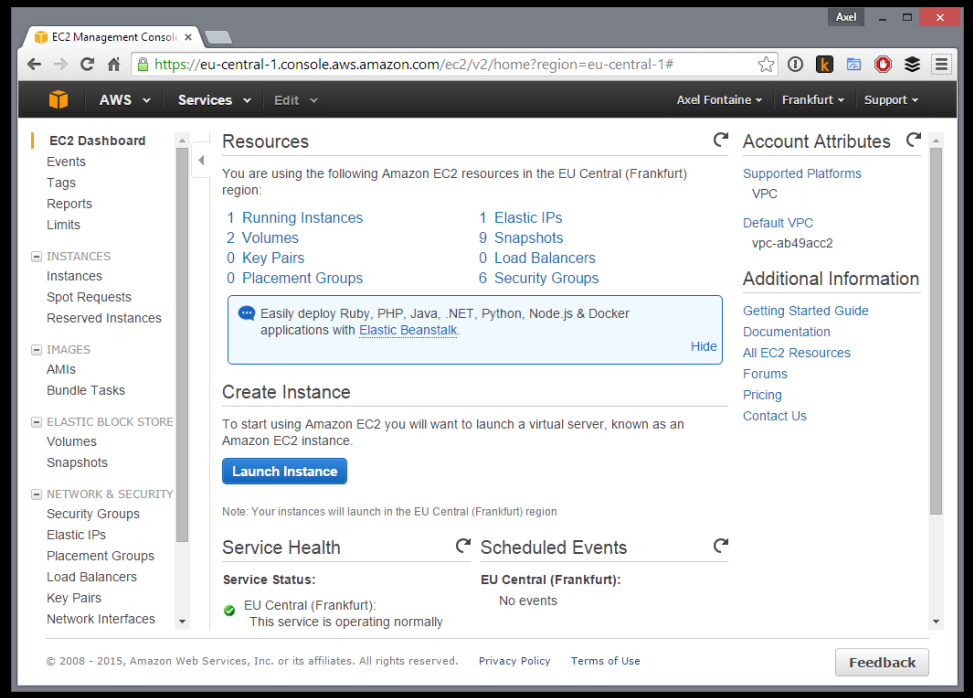
Control Plane

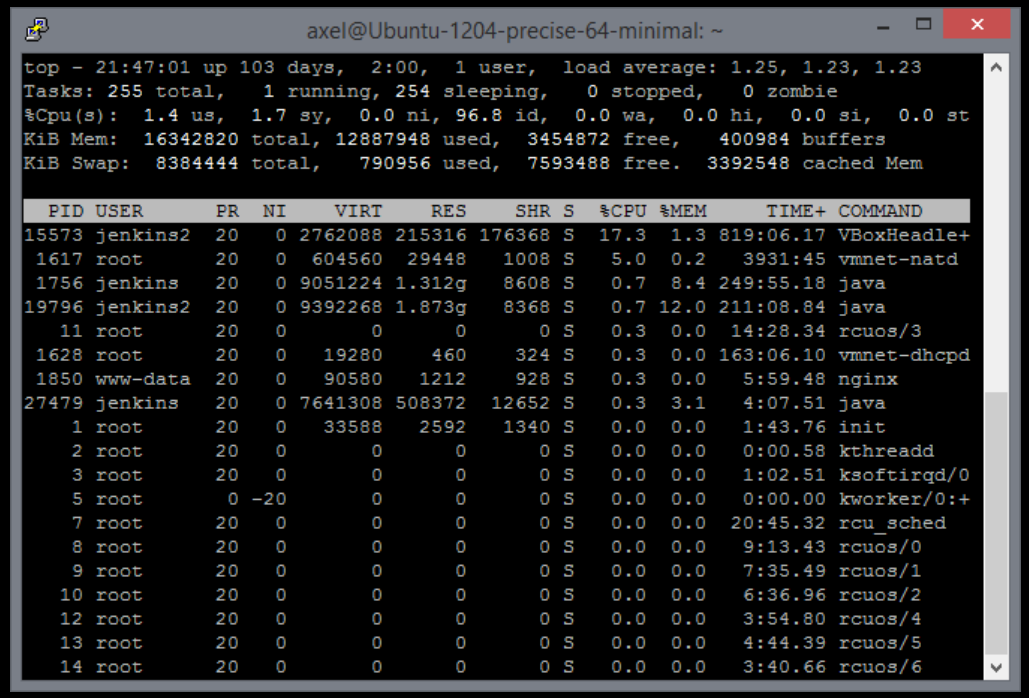


"Advanced Test Reactor" by Argonne National Laboratory - originally posted to Flickr as Advanced Test Reactor Core, Idaho National Laboratory. Uploaded using FlickreviewR. Licensed under CC BY-SA 2.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Advanced_Test_Reactor.jpg#mediaviewer/File:Advanced_Test_Reactor.jpg

Data Plane

boxfuse

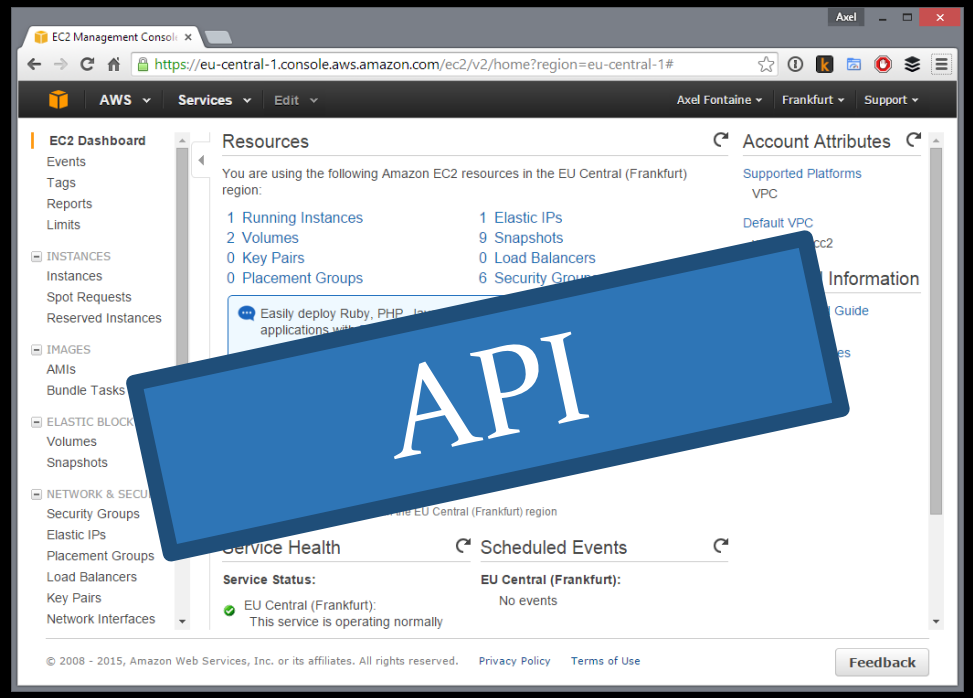


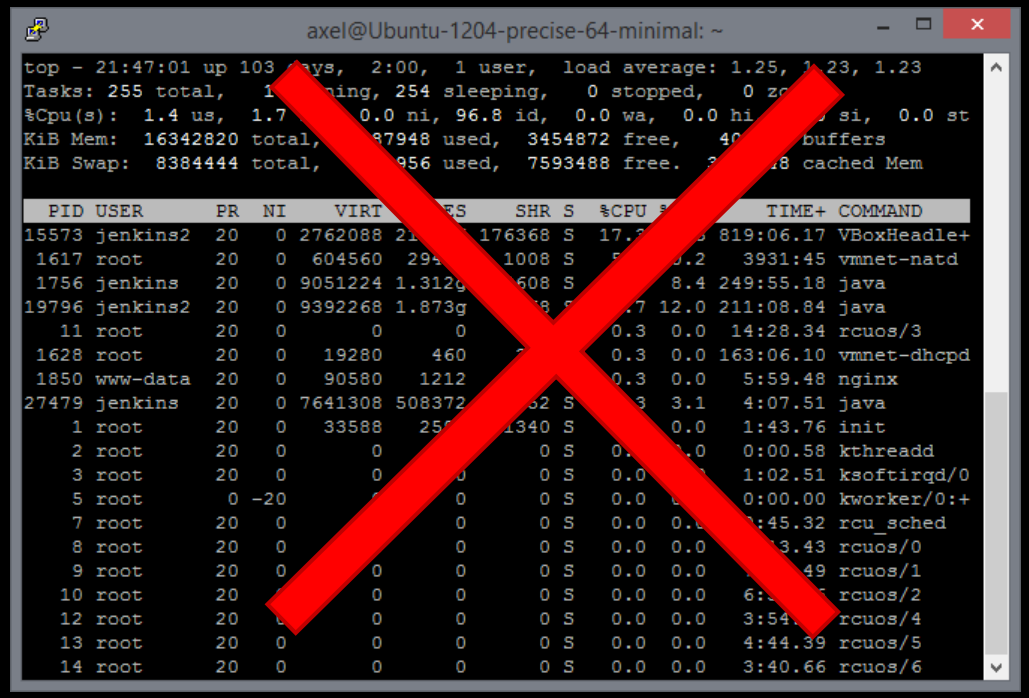


Control Plane

Data Plane

boxfuse



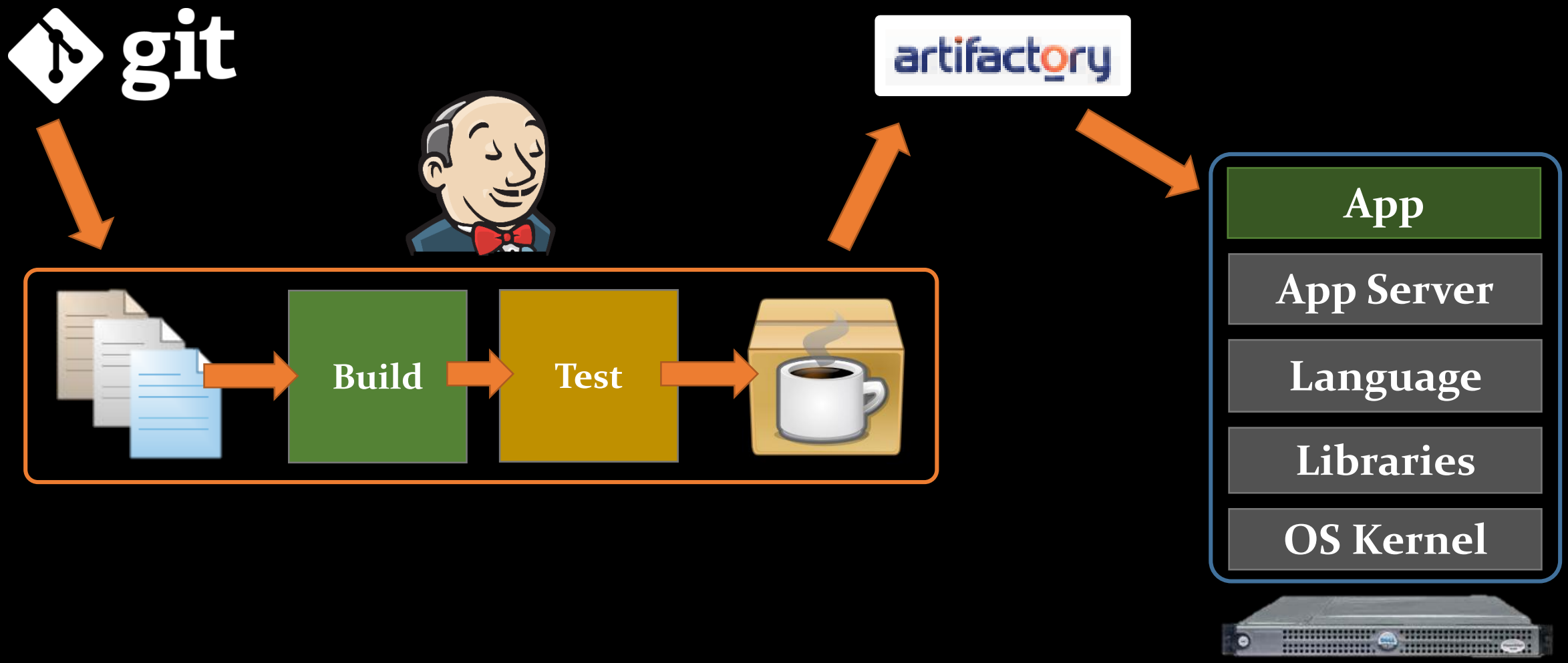


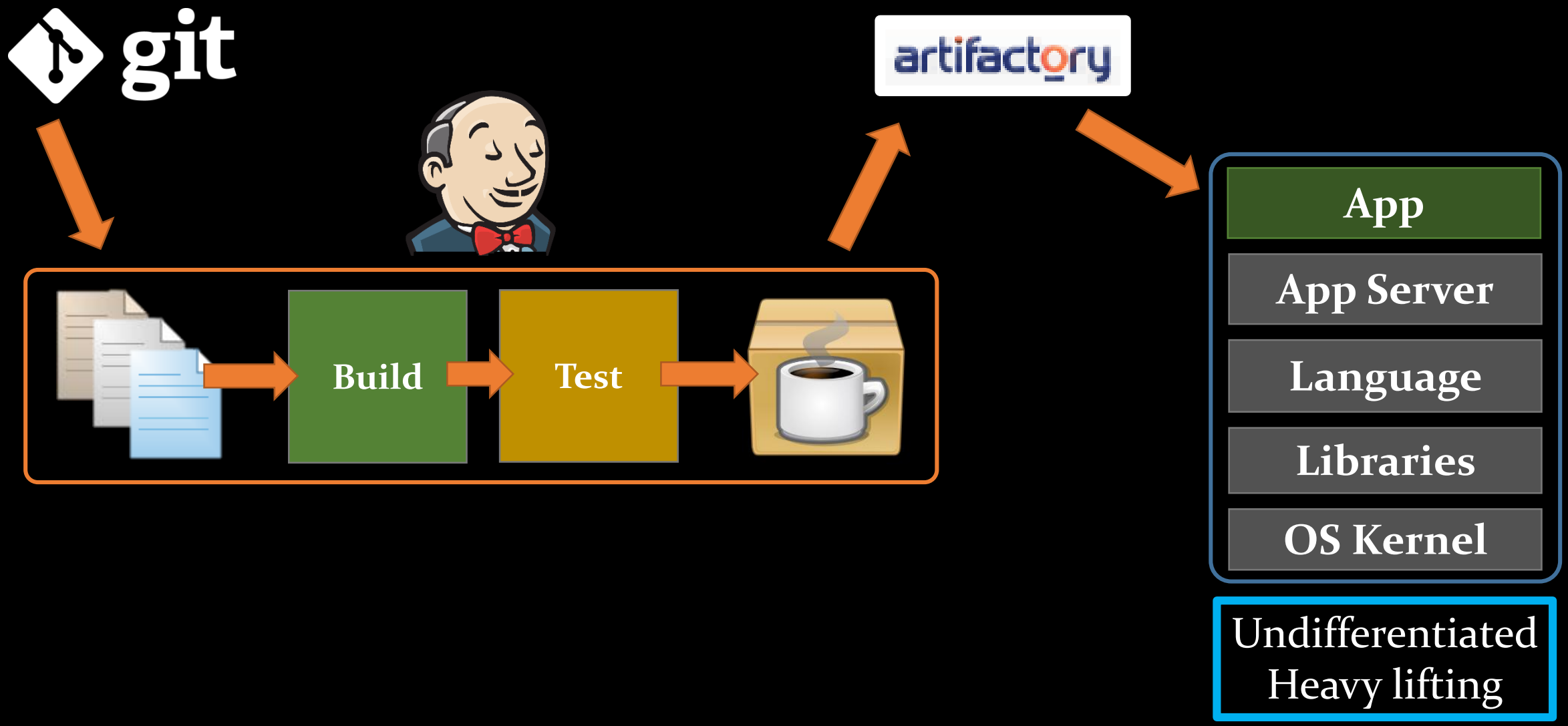
Automated Provisioning

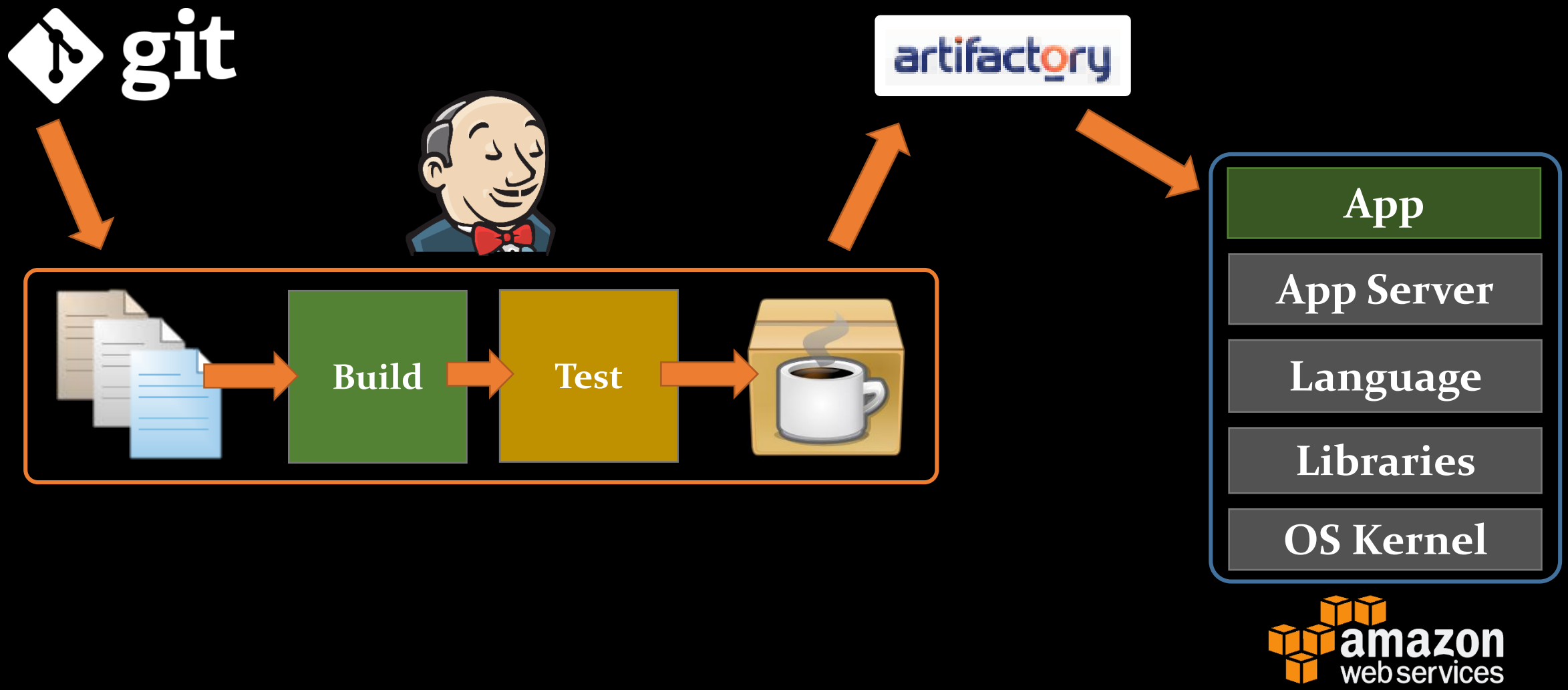
Cost-driven Architectures

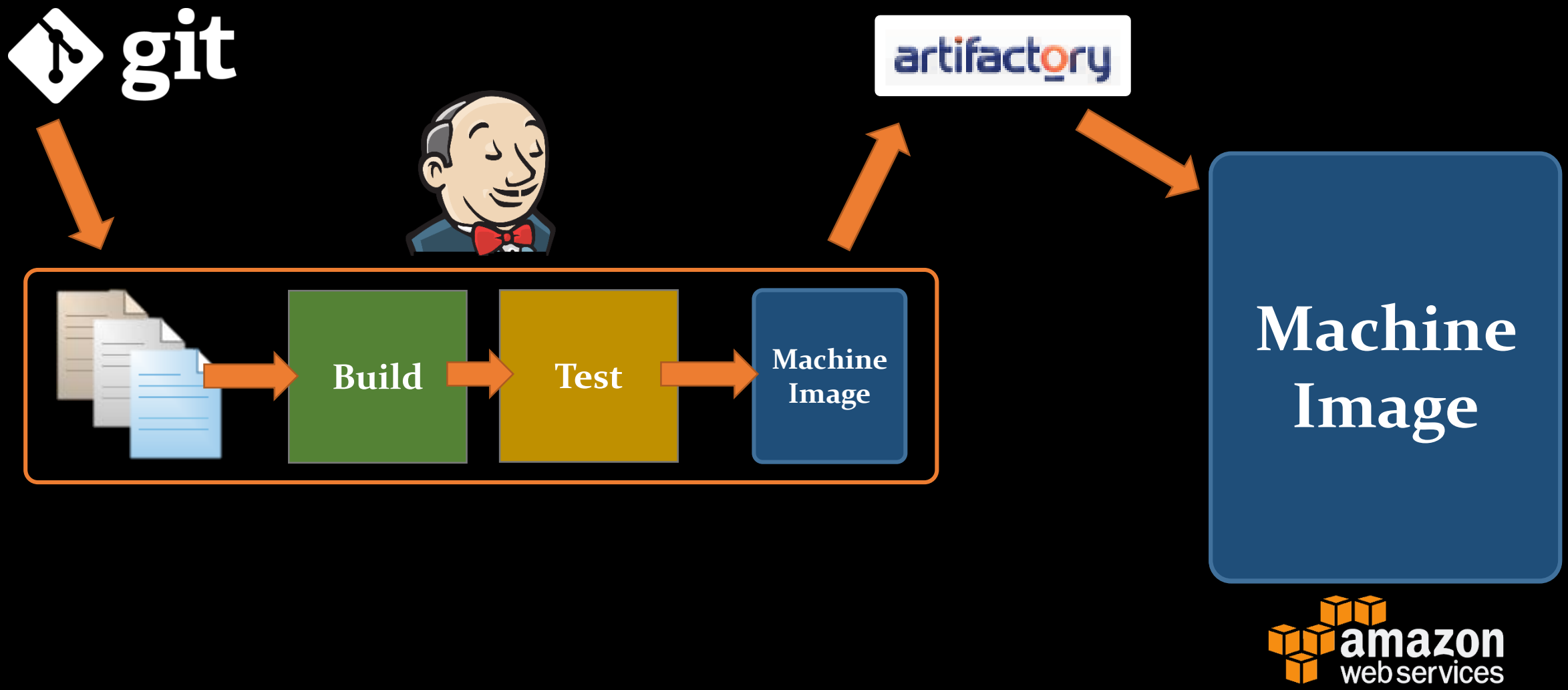
boxfuse

it is time to rethink the faster horse


git
artifactory
Build
Test
App
App Server
Language
Libraries
OS Kernel


git
artifactory
Build
Test
App
App Server
Language
Libraries
OS Kernel
Undifferentiated
Heavy lifting
boxfuse


git
artifactory
Build
Test
App
App Server
Language
Libraries
OS Kernel
amazon
web services
boxfuse


git
artifactory
Build
Test
Machine Image
Machine Image
amazon web services
boxfuse

Machine Image

Machine Image

Machine Image

~~Updates~~

Machine Image

Machine Image

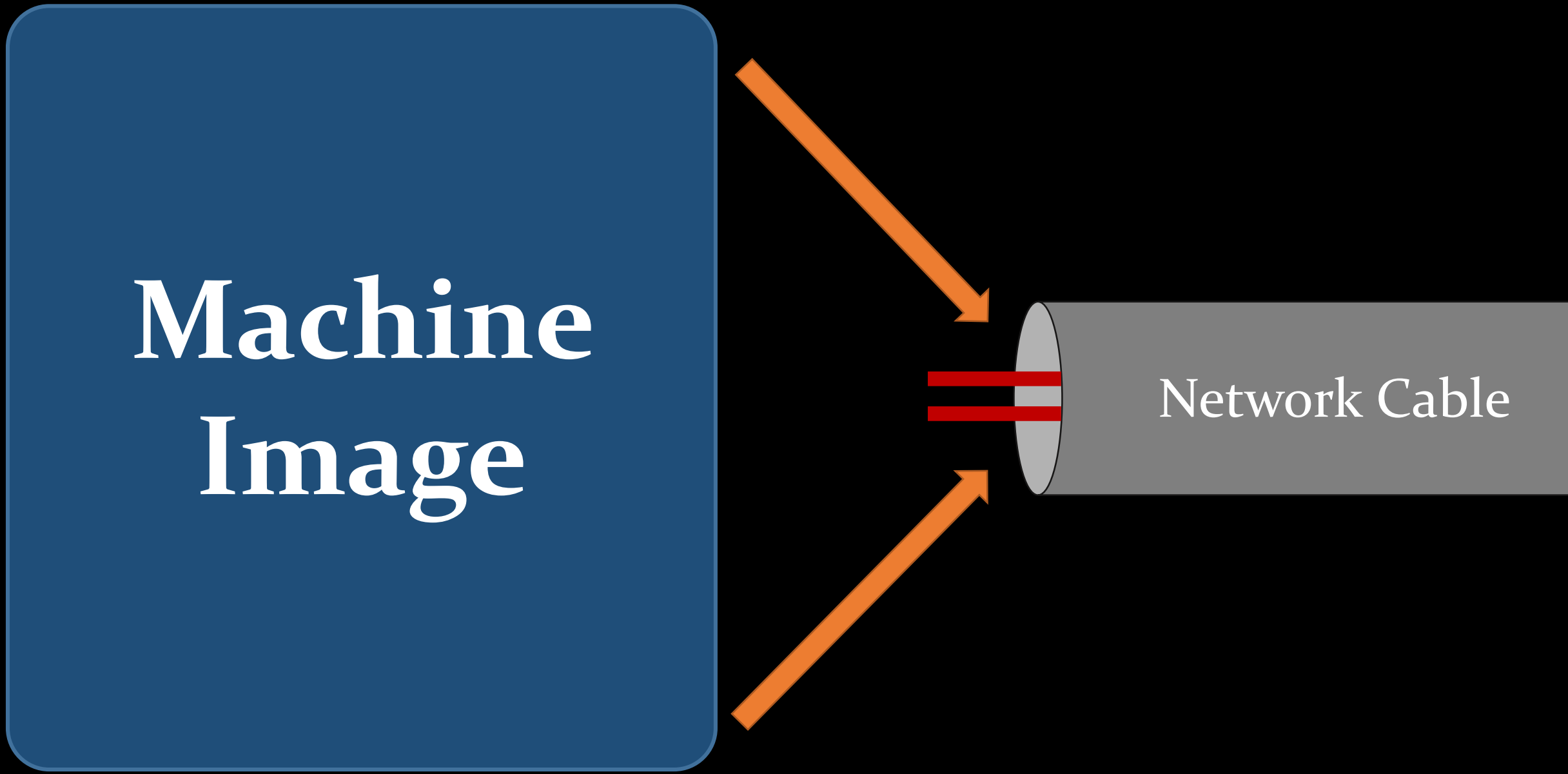
Machine Image

amazon web services

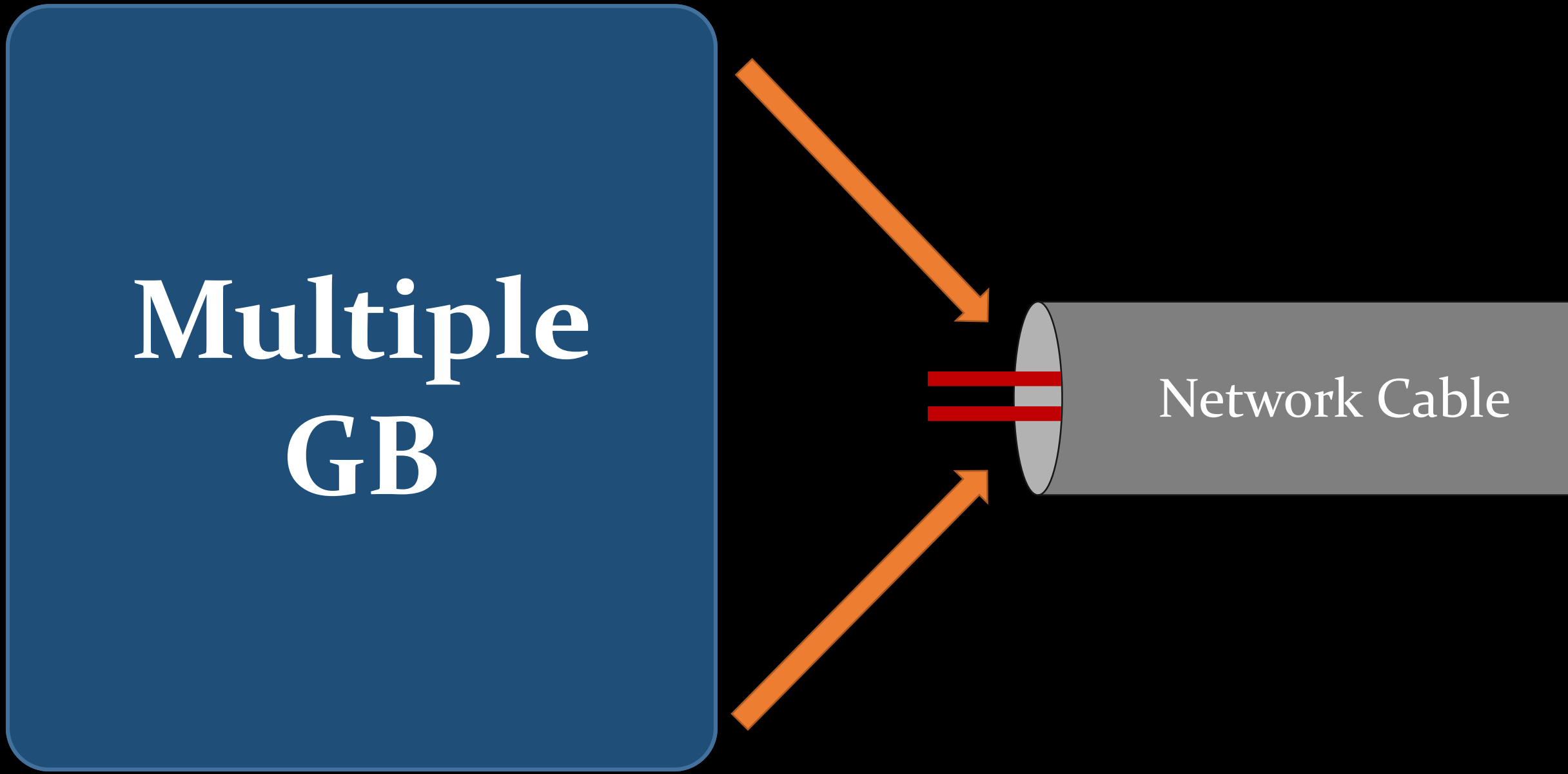
amazon web services

boxfuse

but there is one big problem left …



boxfuse

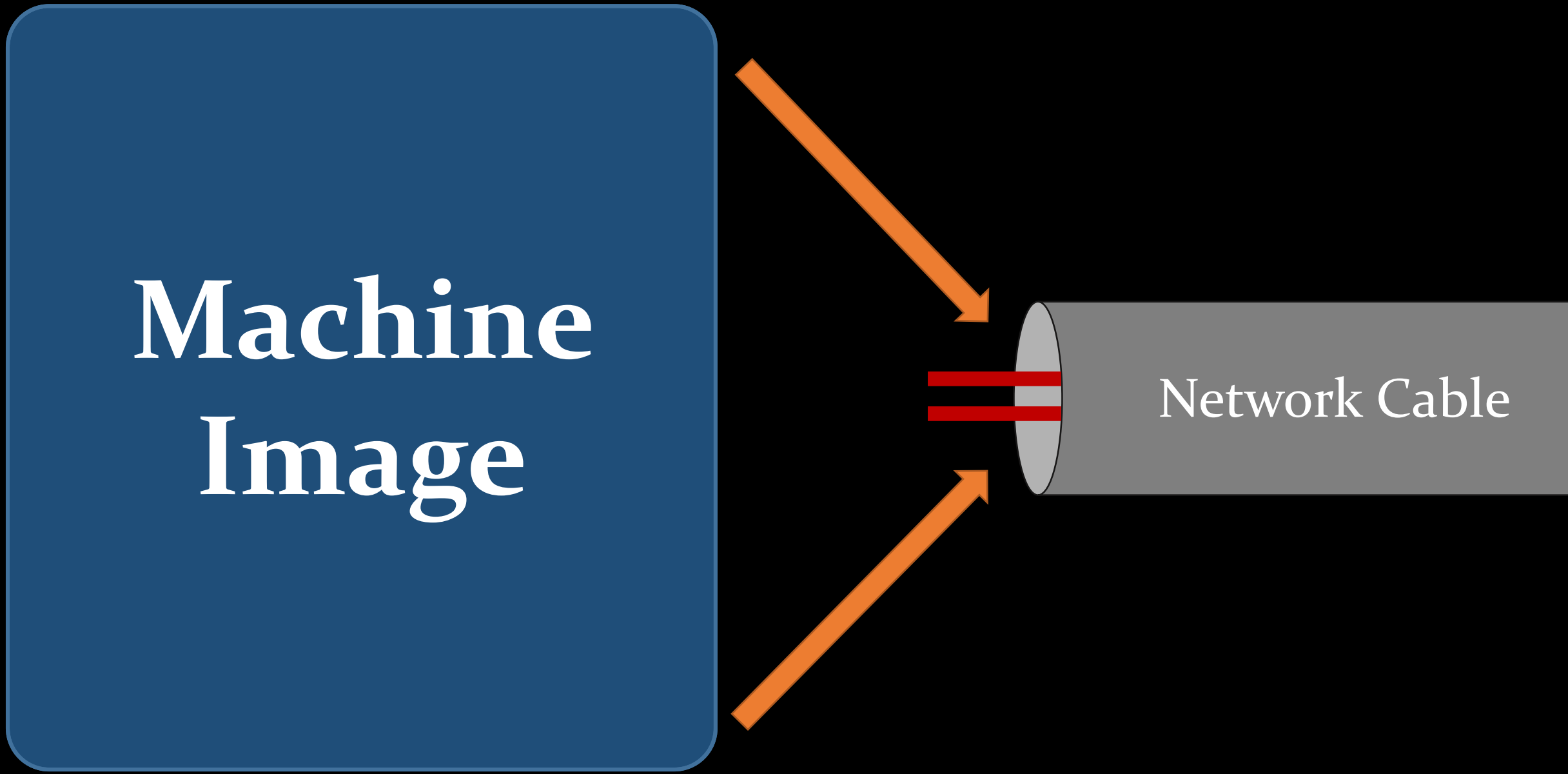

Multiple GB
Network Cable

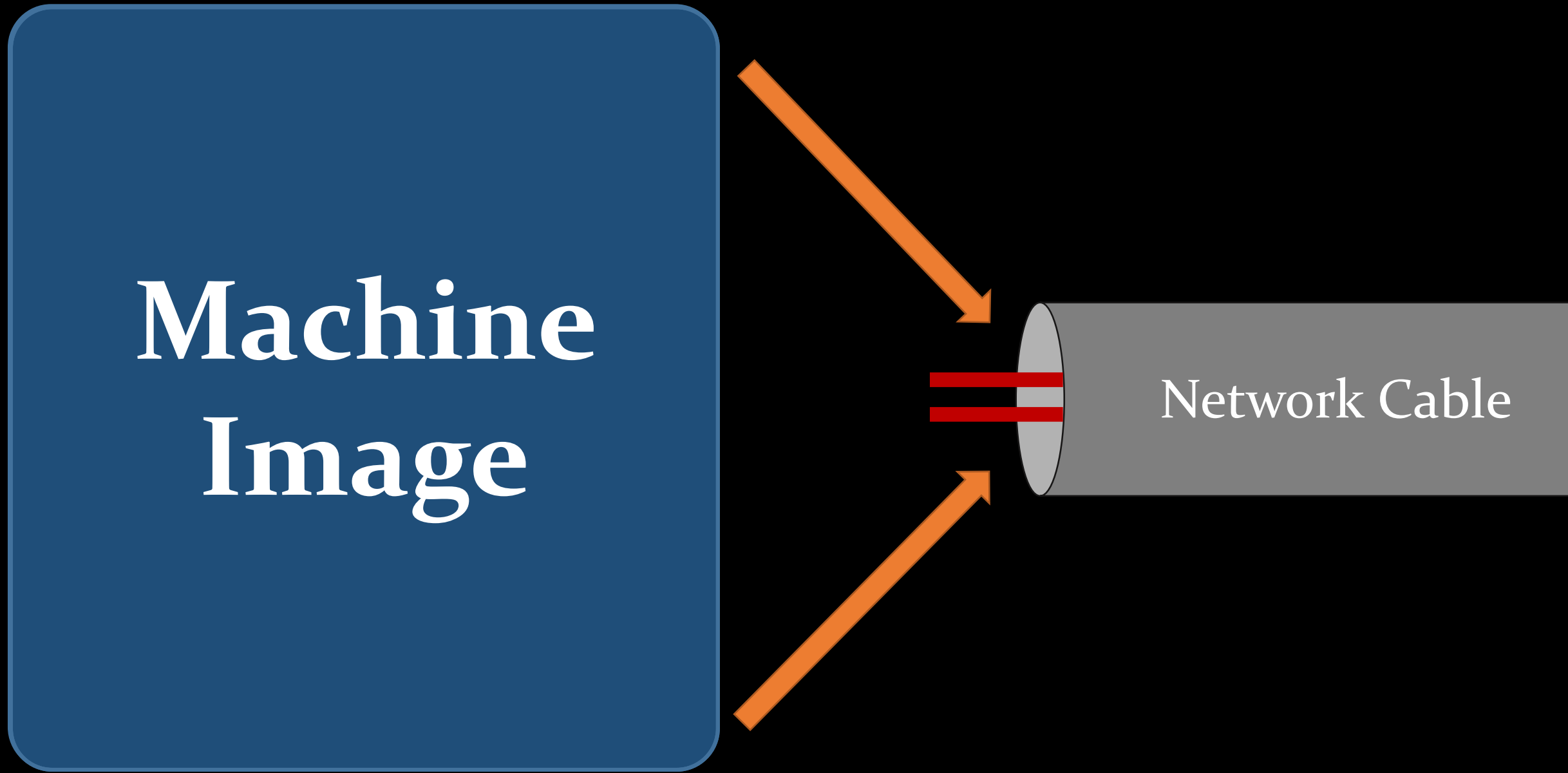
Running servers in production should be like going backpacking. You take the bare minimum with you. Anything else is going to hurt.

A Wise Man

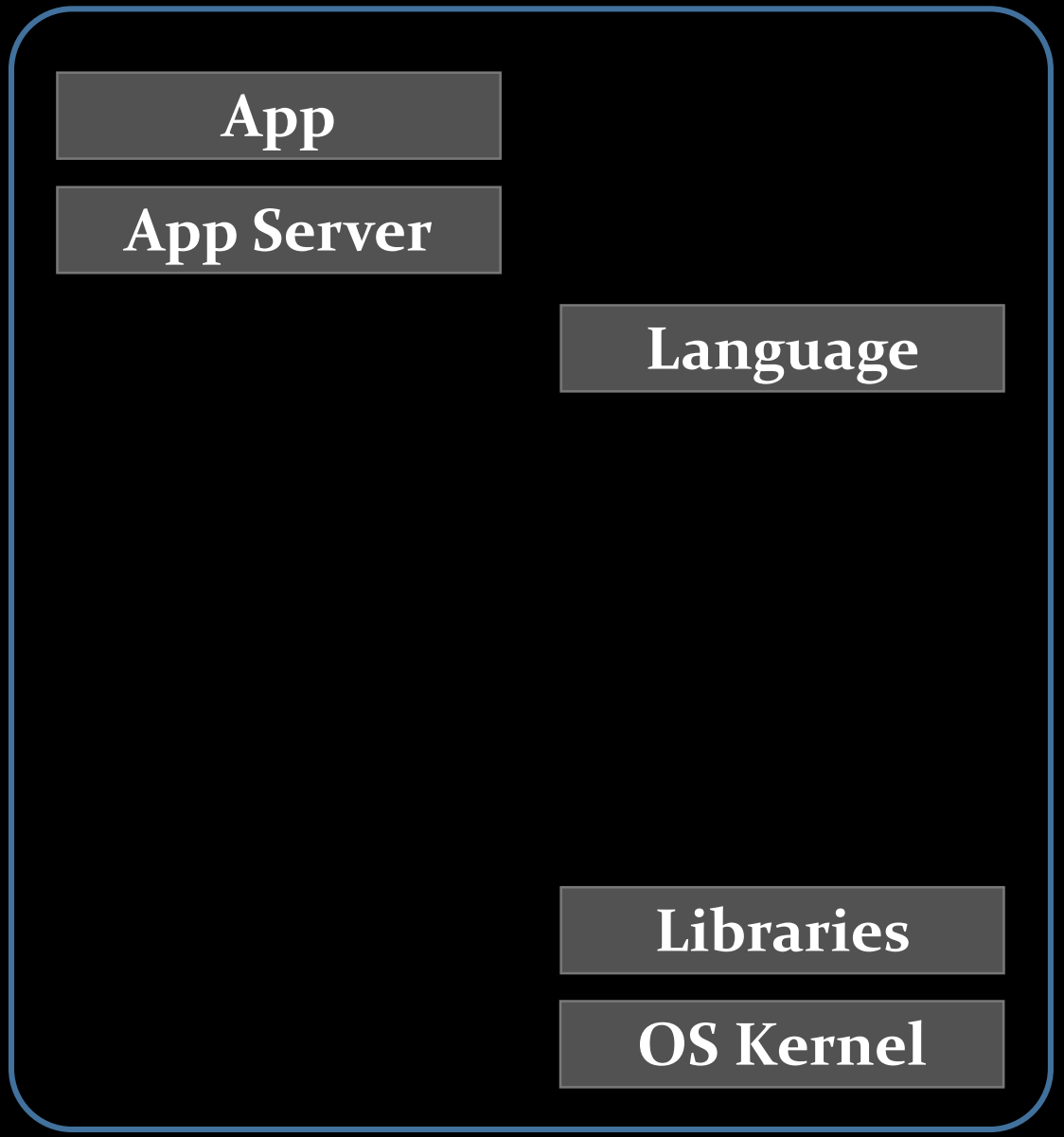
boxfuse

what is really adding business value ???


Machine Image
Network Cable



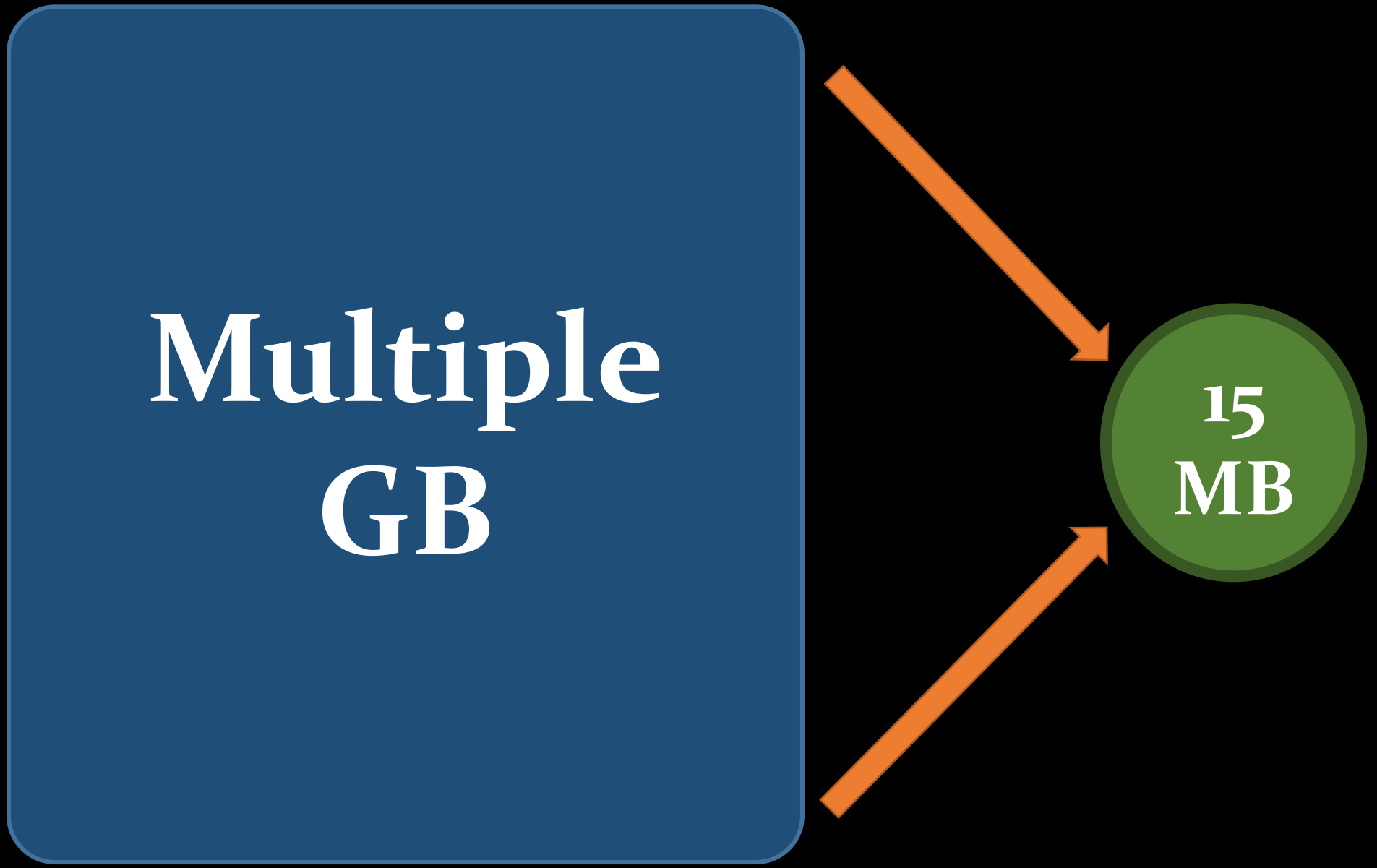
boxfuse



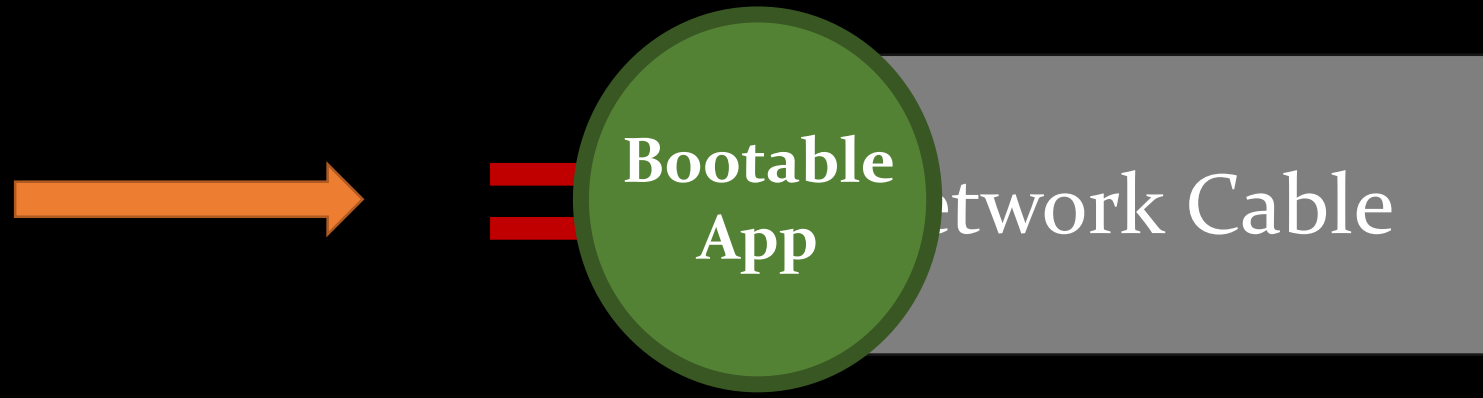
Bootable App

boxfuse

15
MB

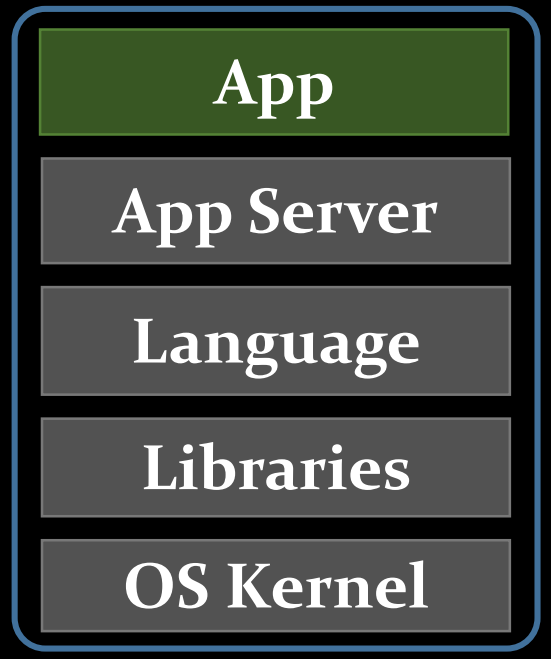


boxfuse



boxfuse

who is this for ???



12-factor app

boxfuse

demo

What are the implications ???

Focus shift

Instance  Service

Individual instances become disposable

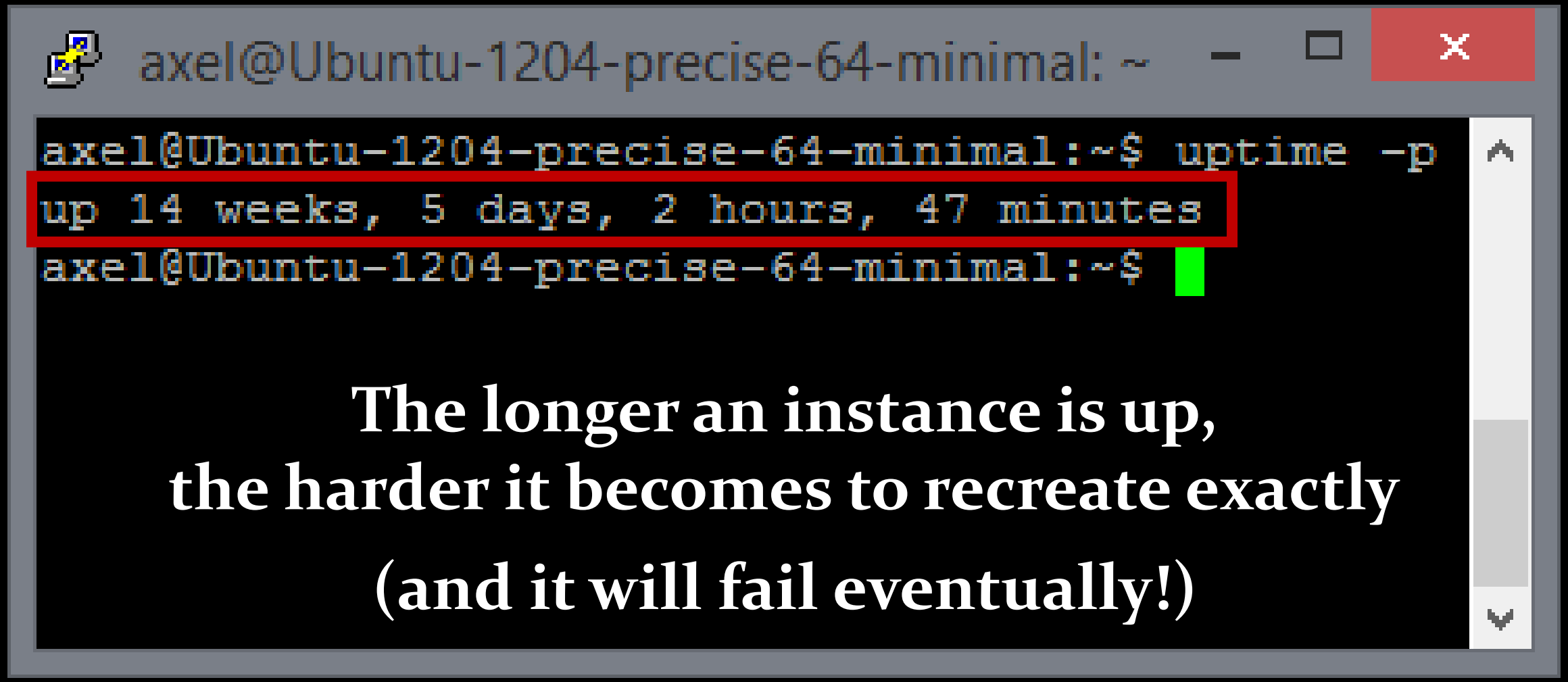
Treat servers like cattle instead of pets

boxfuse

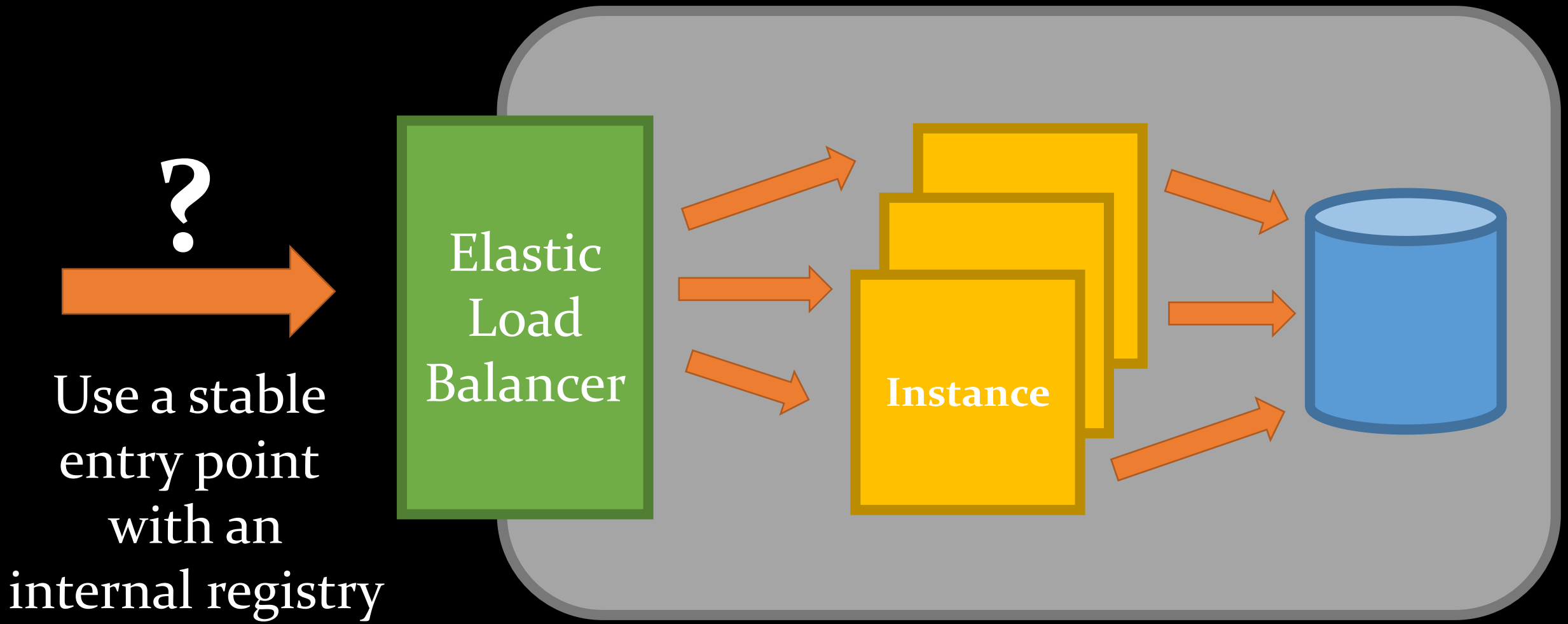
for servers is dead!

boxfuse

high uptime is a liability



How to solve service discovery ?



Use a stable entry point with an internal registry

What about security ?

When was the last time your toaster got hacked?

boxfuse

What about security ?

Complexity is the Enemy of Security

boxfuse

What about security ?

- Smallest possible attack surface
- Vastly reduced implications due to low uptime and transient nature of instances
- Very difficult to exploit other systems because essential tooling is missing

what about configuration ???

- Bake as much configuration as possible for all environments directly in the Bootable App

- Use environment detection and auto-configuration

what about configuration ???

- Bake as much configuration as possible for all environments directly in the Bootable App

Key	Value
JDBC_URL	jdbc:...
ENV	prod

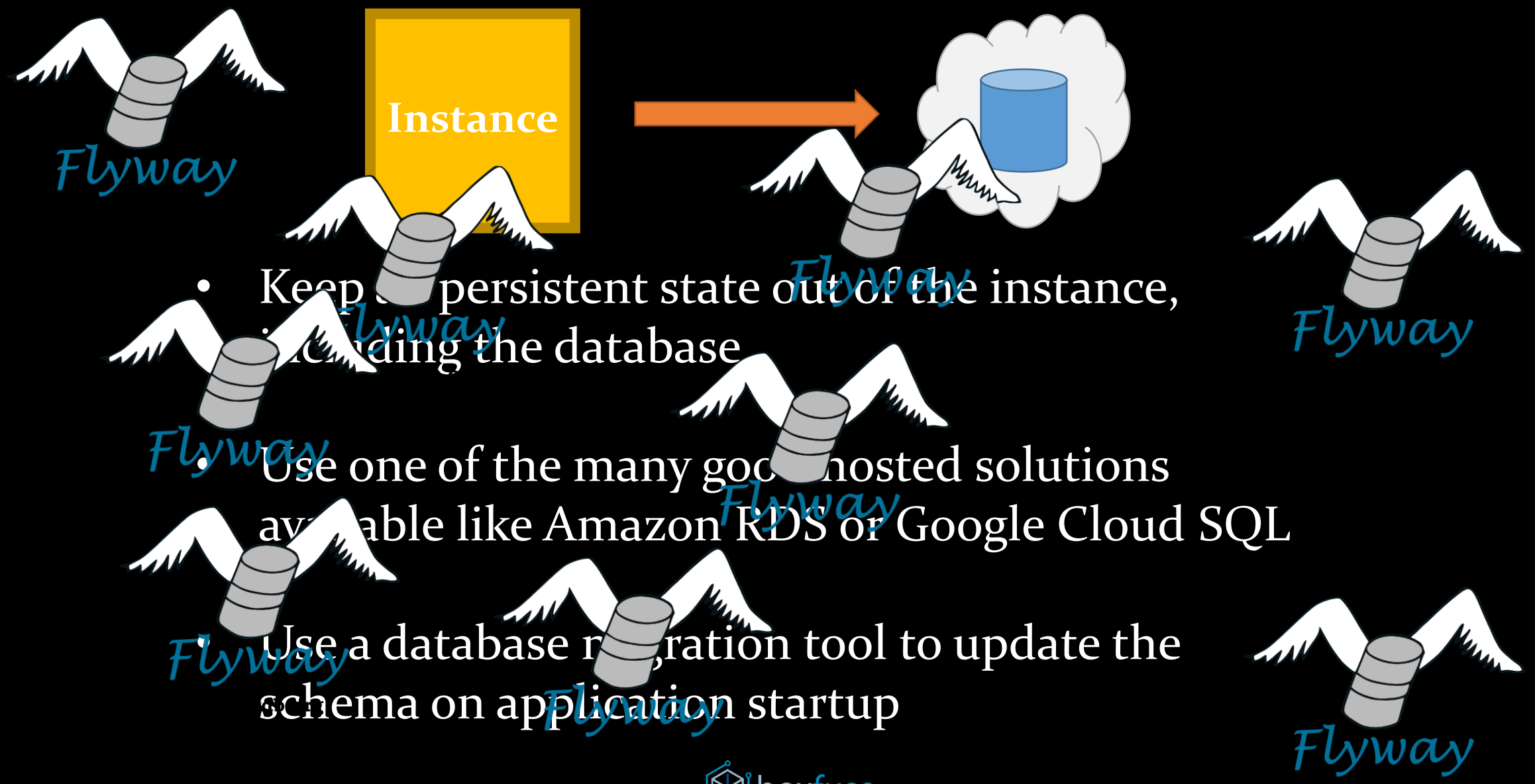
- Use environment detection and auto-configuration

- Pass remaining configuration at startup and expose it as environment variables

amazon web services

boxfuse

what about the database ???



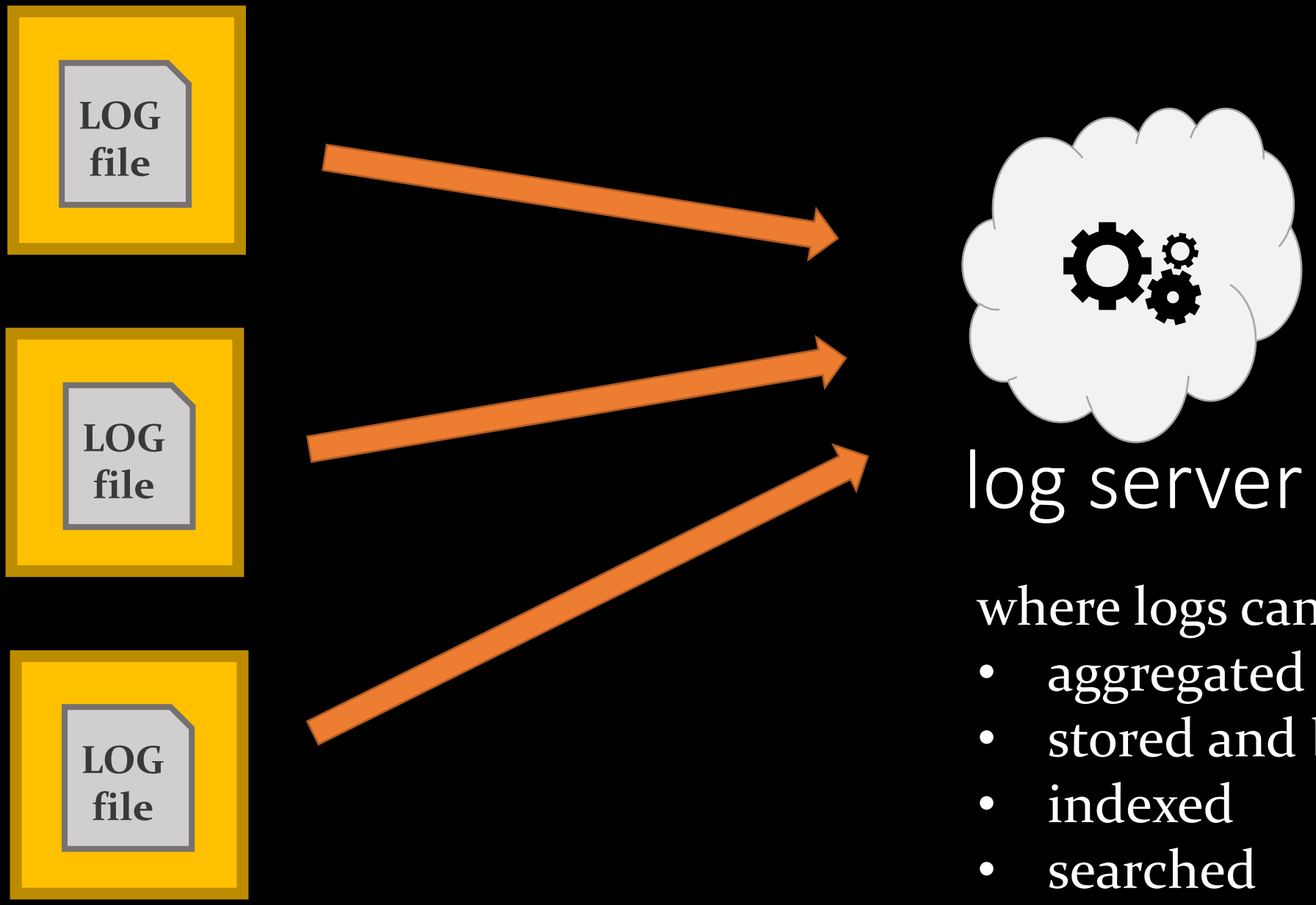
- Keep all persistent state out of the instance, including the database
- Use one of the many good hosted solutions available like Amazon RDS or Google Cloud SQL
- Use a database migration tool to update the schema on application startup

what about the logs ???

~~ssh me@myserver1~~
~~tail -f server.log~~

~~ssh me@myserver2~~
~~tail -f server.log~~

~~ssh me@myserver3~~
~~tail -f server.log~~



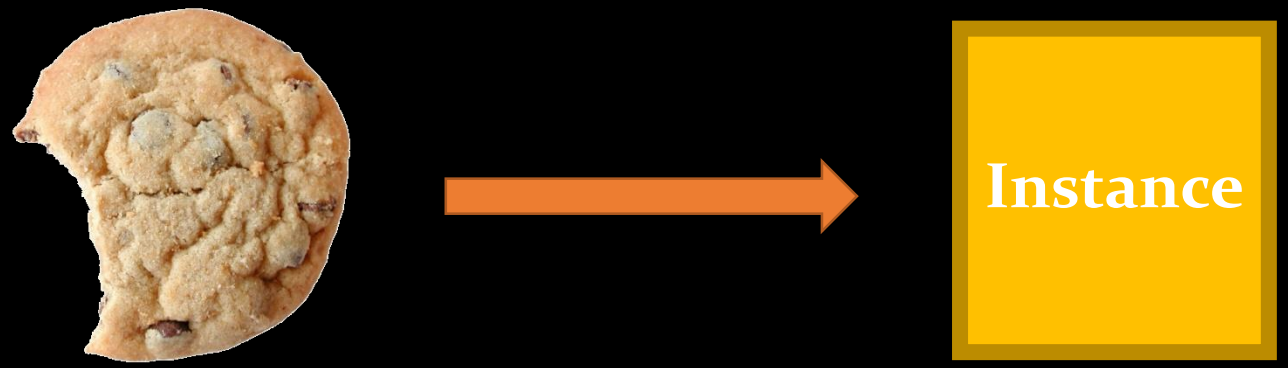
log server

where logs can be

- aggregated
- stored and backuped
- indexed
- searched

boxfuse

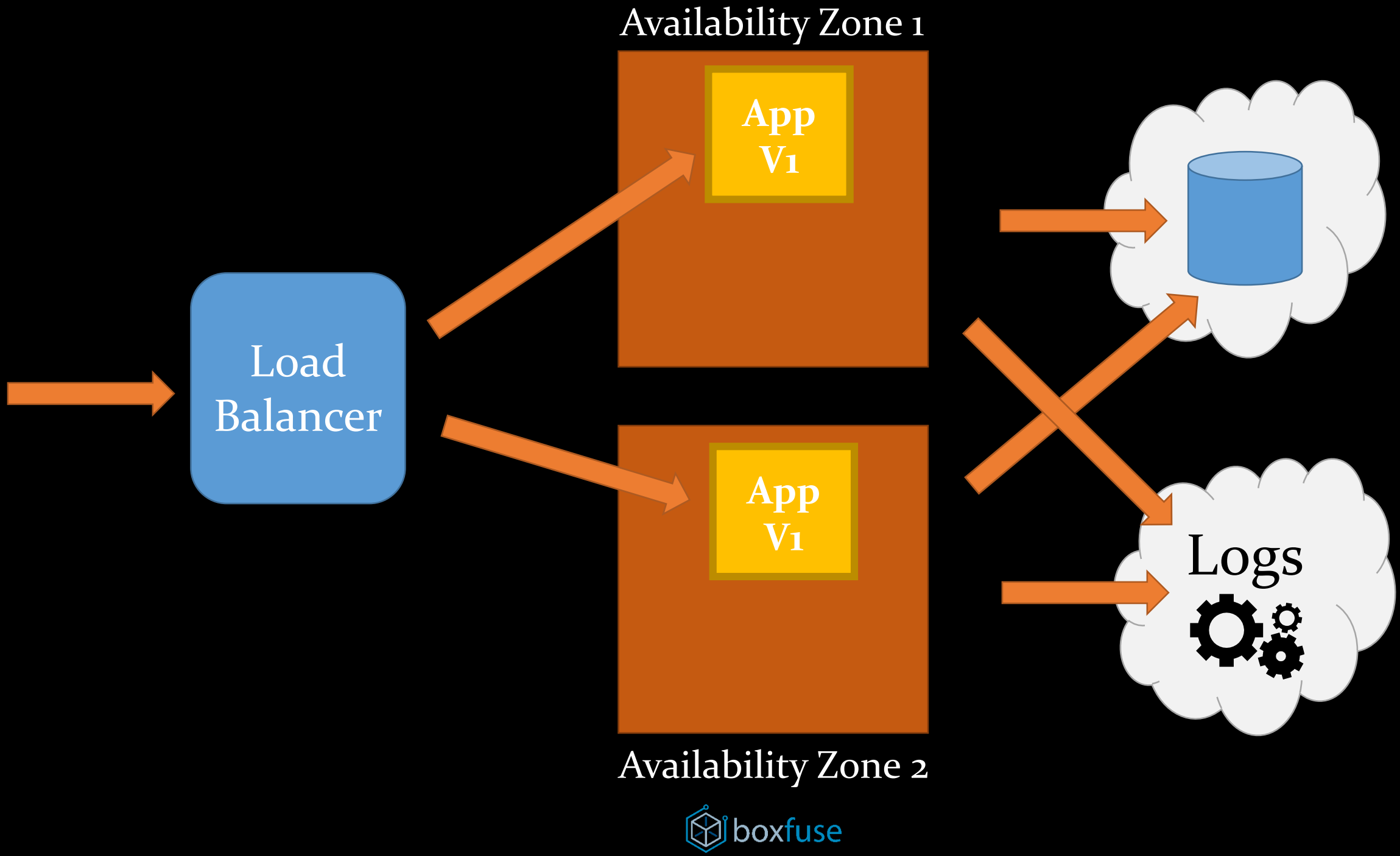
what about sessions ???

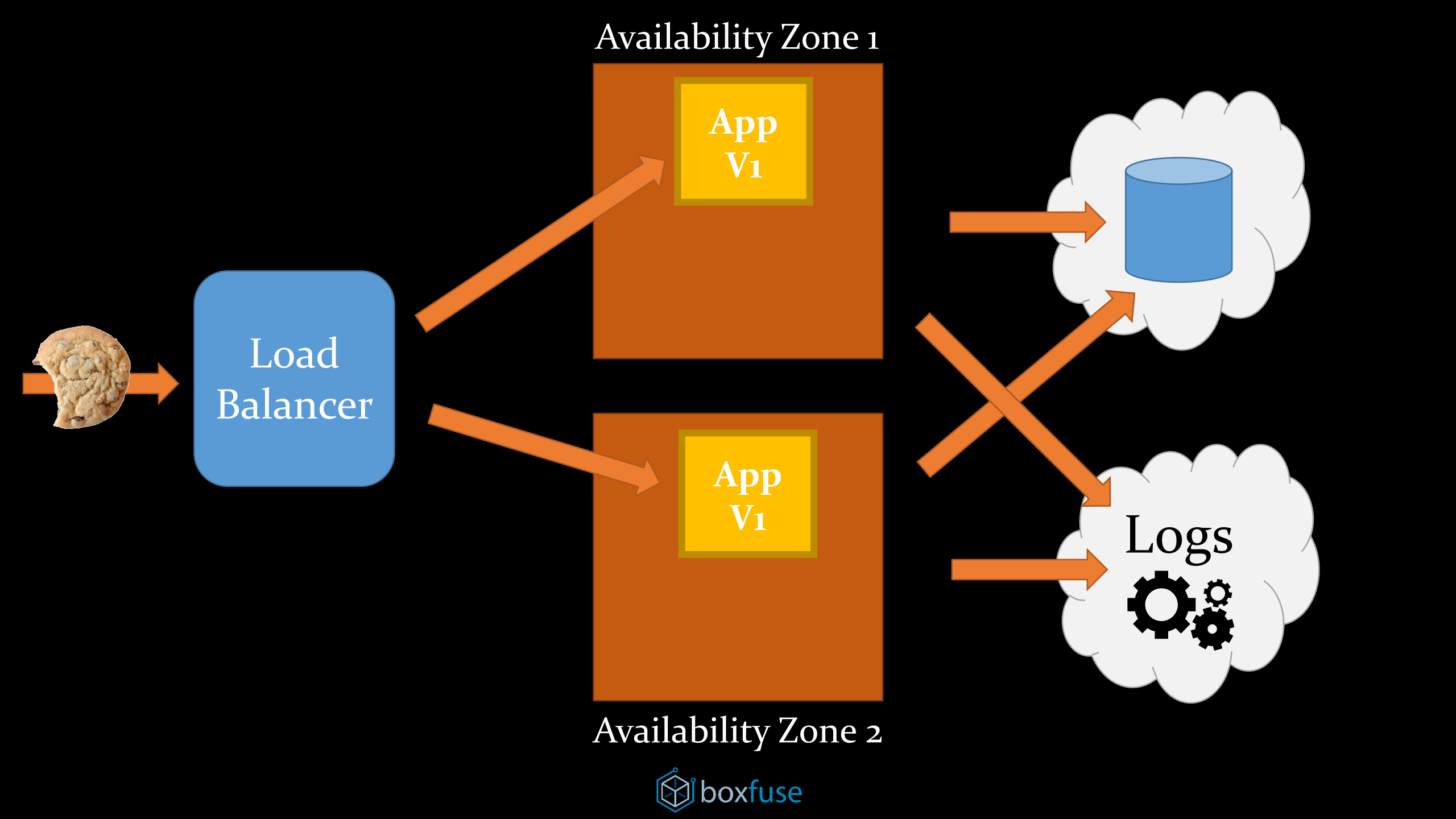


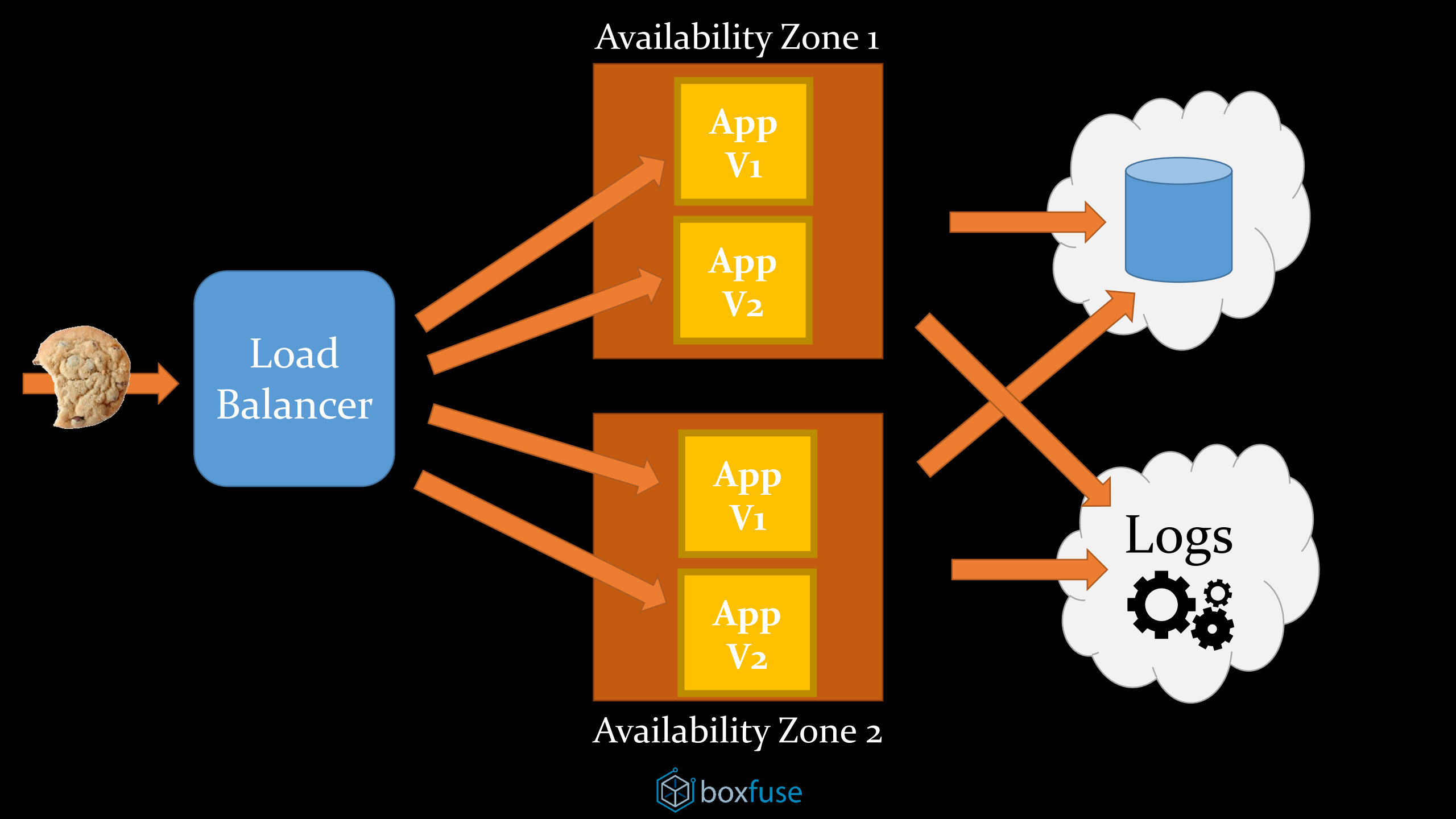
Keep session in an encrypted and signed cookie

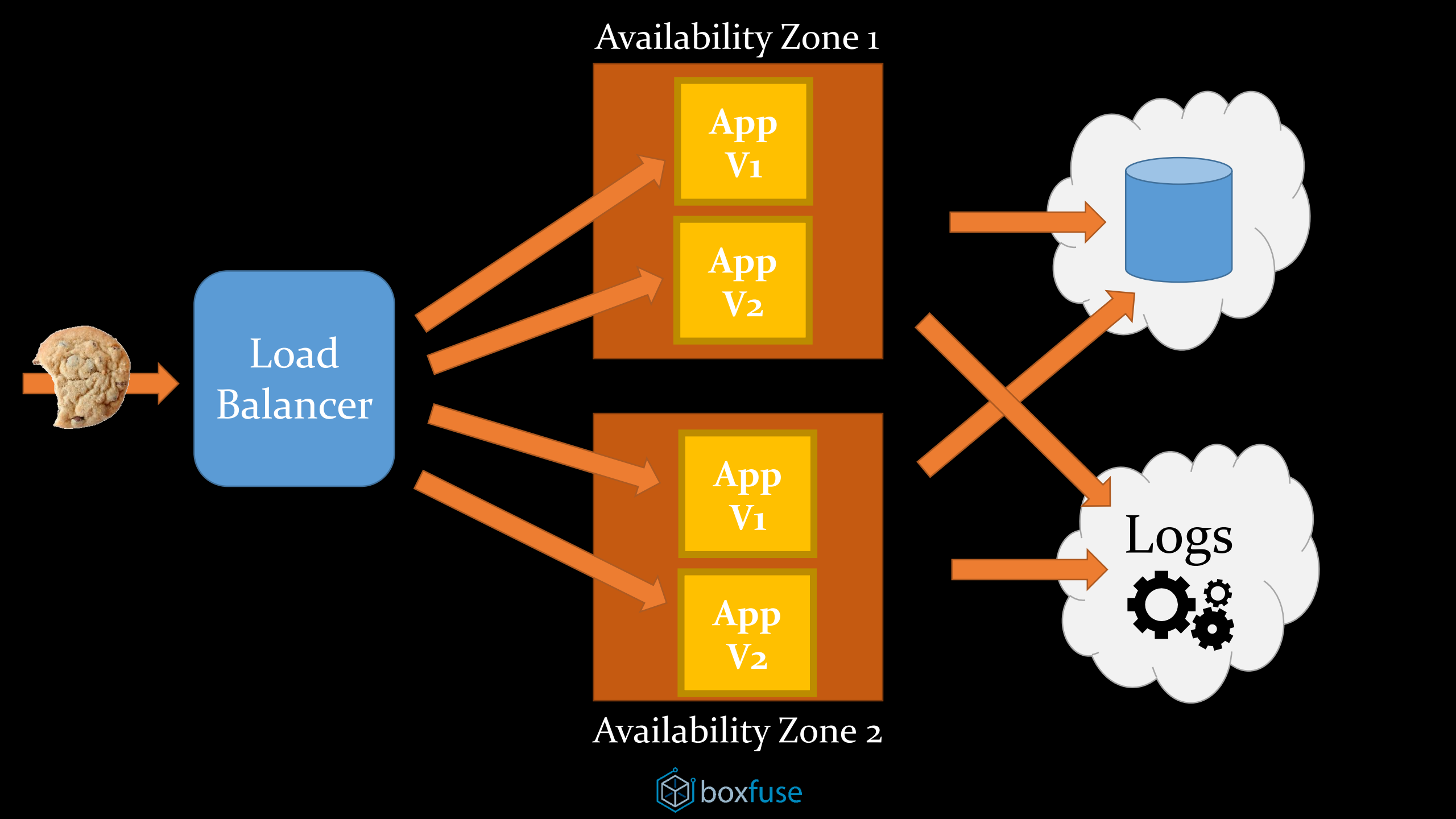
- avoids session timeouts
- avoids server clustering & session replication
- avoids sticky sessions & server affinity

what about rolling out new versions ???


Availability Zone 1
App
V1
Load
Balancer
App
V1
Logs
Availability Zone 2
boxfuse


Availability Zone 1
App
V1
Load
Balancer
App
V1
Logs
Availability Zone 2
boxfuse


Availability Zone 1
App V1
App V2
Load Balancer
App V1
App V2
Logs
Availability Zone 2
boxfuse


Availability Zone 1
App V1
App V2
Load Balancer
App V1
App V2
Logs
Availability Zone 2
boxfuse

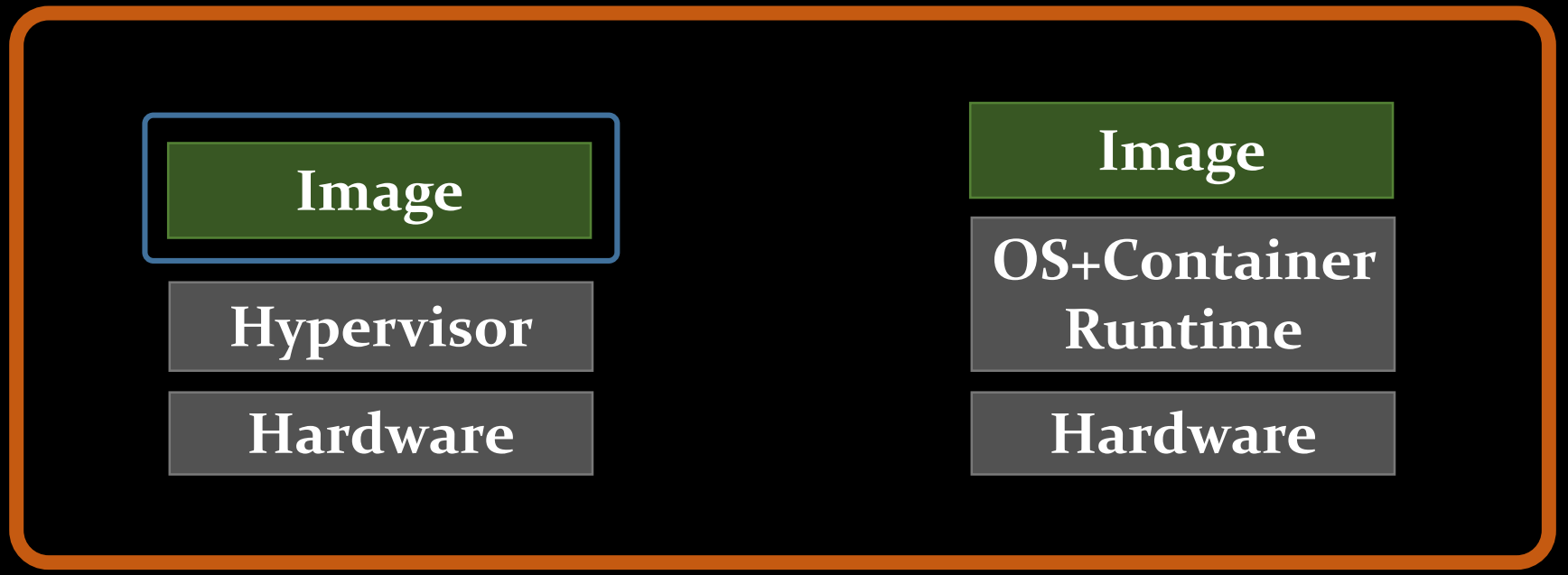
what about containers ???
(as in OS-level virtualization)

understanding modern CPUs

Both Intel and AMD have hardware support for virtualization

- isolation
- performance penalty

on prem

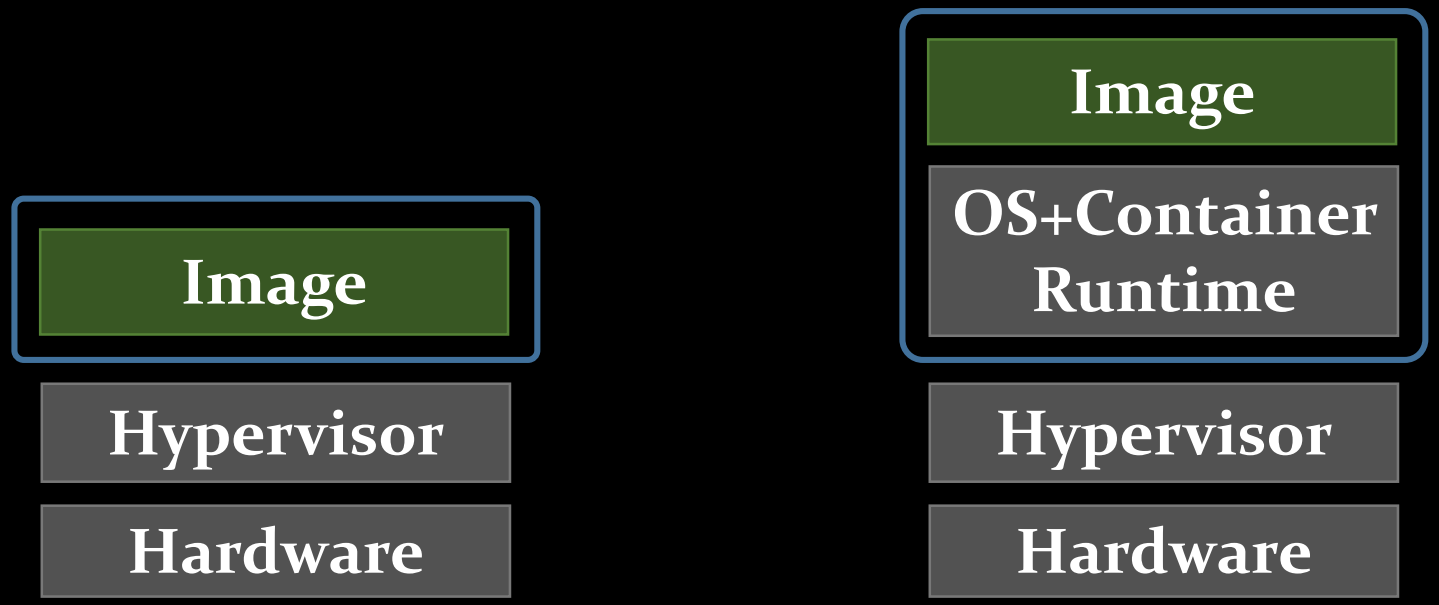


your responsibility

VM

Container

cloud

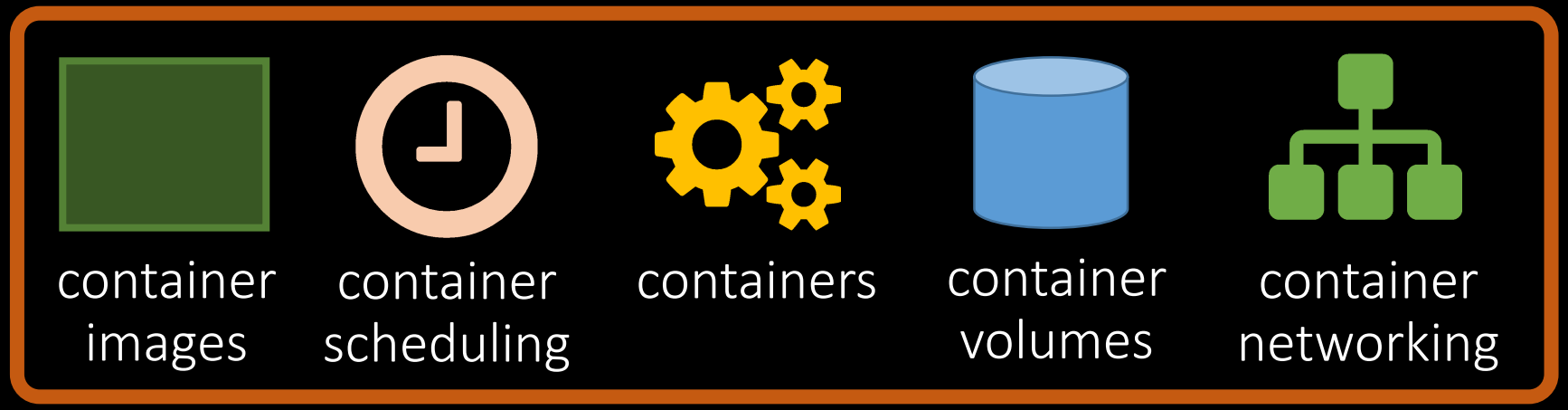


VM

Container

boxfuse

cloud



your responsibility

cloud responsibility

boxfuse

1 month of t2.nano

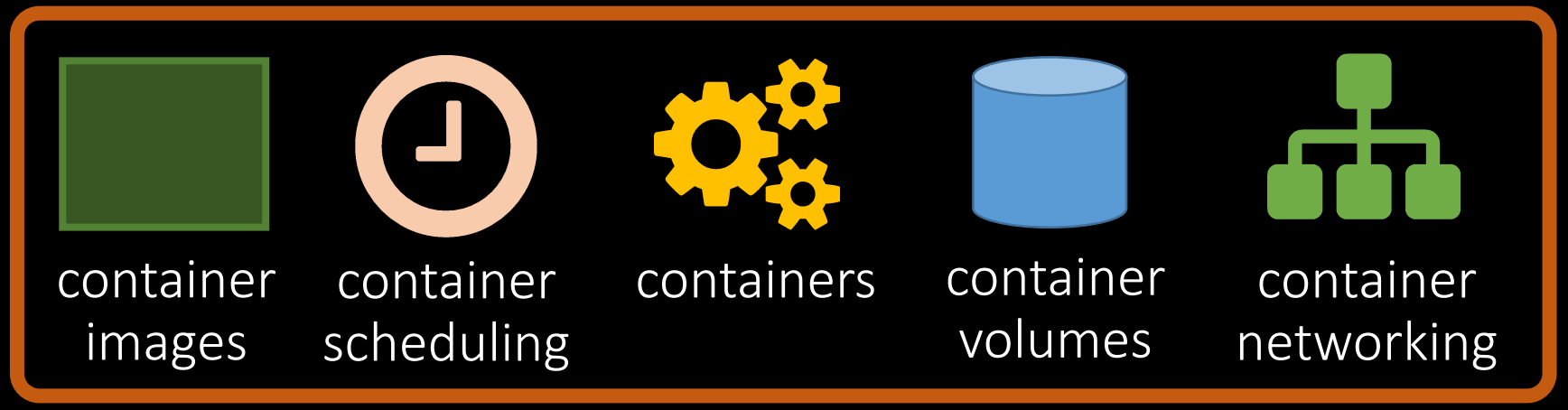
boxfuse

1 hour of t2.nano

boxfuse

cloud

Only makes sense if you cannot afford 0.5 Rappen/hour granularity



your responsibility

cloud responsibility

boxfuse

summary

- One immutable unit
- Regenerated after every change
- Promoted from Environment to Environment

Classic Mistake: Build per Environment

boxfuse

- One immutable unit
- Regenerated after every change
- Promoted from Environment to Environment
- Use Minimal Images
- Focus on Cost in your architecture

Classic Mistake: Build per Environment

boxfuse

boxfuse

boxfuse.com

THANKS

AXEL FONTAINE
@axelfontaine

I'LL BE BACK

boxfuse

boxfuse.com