Linux distributions, lifecycles, and containers

Adam Samalik, Red Hat
@adsamalik
Developers want variety and new versions
Operators
want packages, auditability, lifecycle, support
Dev and Ops are very different
yet they need to work together
Isn't this just packaging?

That's what Linux distributions do.
Packaging makes software integrated, tested, updated, and easily installable.
Lifecycle

brings an over-time stability
to the diverse
open source world.
Upstream lifecycle diversity

- Library foo
- Library foo even better
- Language runtime B
- Language runtime A
- Application v2
- Application v1

maintenance timeline
Linux distribution lifecycle

- Library foo better
- Library foo
- Language runtime B
- Language runtime A
- Application v2
- Application v1

Maintenance timeline
Linux distribution lifecycle

Fedora 27

Fedora 28

maintenance timeline
Lifecycles of different Linux distributions

- CentOS
- Fedora
- Arch Linux

maintenance timeline
Sounds good for ops.
Packages, lifecycle, updates, transparency, ...
But it's monolithic.

Developers or existing apps might be limited.
Containers?

Do they make both dev and ops happy?
Containers are isolated and portable.
But containers are just isolated and portable. They won't magically fix bugs or security issues for you.
We need:
new versions and variety for developers with the qualities required by operators.
Modularity separates the lifecycles of different pieces of a Linux distribution.
Linux distribution lifecycle

Fedora 27

Fedora 26

maintenance timeline
Fedora Modularity
Traditional releases before Modularity

Fedora 26
nodejs-6.rpm

Fedora 27
nodejs-8.rpm
Fedora Modularity
Fedora 28 with multiple versions

Fedora 26
nodejs-6.rpm

Fedora 27
nodejs-8.rpm

Fedora 28
nodejs 6 stream
nodejs-6.rpm
nodejs 8 stream
nodejs-8.rpm
nodejs 10 stream
nodejs-10.rpm
Fedora Modularity
Multiple versions & independent lifecycles
Fedora Modularity
Multiple versions & independent lifecycles

Fedora 27
nodejs-8.rpm

Fedora 28
  nodejs 6 stream
  nodejs-6.rpm
  nodejs 8 stream
  nodejs-8.rpm
  nodejs 10 stream
  nodejs-10.rpm

Fedora 29
  nodejs-6.rpm
  nodejs-8.rpm
  nodejs-10.rpm
Packages are the core building blocks of Linux distributions.
Modules are logical groups of packages on independent lifecycles.
Defaults mean that you can choose a specific version only when you want to.
Updates will respect your choice and won’t automatically upgrade to a different stream.
Demo:
Managing modules in Fedora using DNF
Containers again
The true container benefits:

They run almost anywhere.

Compose + testing can be done up front.
3rd party container registries are handy, you just find a container and run it.

That's perfectly fine, isn't it? There's no risk or anything, right?
3rd party container registries are handy, you just find a container and run it. That's perfectly fine, isn't it? There's no risk or anything, right?

https://kromtech.com/blog/security-center/cryptojacking-invades-cloud-how-modern-containerization-trend-is-exploited-by-attackers
“… By pushing malicious images to a Docker Hub registry and pulling it from the victim’s system, hackers were able to mine 544.74 Monero, which is equal to $90000…”
Back to the true container benefits:

They run almost anywhere.

Compose + testing can be done up front.
Build custom containers
with Linux distributions.

Leveraging both:
the Linux distributions benefits (packaging, lifecycle)
and container benefits (portability, isolation).
What about the underlying OS when my apps run in containers? Should I care?
You definitely need to care about the OS for security, performance, and new hardware compatibility.

But it doesn't need to be your pet.
With apps in containers, the OS can be immutable.
Traditional upgrade

from orange to green.
Traditional upgrade from orange to green.
rpm-ostree upgrade
from orange to green.
rpm-ostree upgrade from orange to green.
rpm-ostree upgrade
from orange to green.
Fearless upgrades for your server and workstation.
Linux distributions & Modularity
packaging & lifecycle

Containers
"just" portable & isolated

CoreOS and Silverblue
fearless upgrades

Adam Samalik, @adsamalik