

OpenPrinting



# Chiselled Ubuntu containers

**Valentin Viennot – Canonical**

**September 14, 2022**

# How and why (Ubuntu) distroless?



## Provenance + Security concerns with Open Source Software

- Containerisation is not enough to secure an application
- Abstracting dependencies also abstracts vulnerabilities
- Layering mechanism  $\Rightarrow$  many containers based on the same content
- Keeping content up-to-date with containers isn't straightforward

# How and why (Ubuntu) distroless?



# How and why (Ubuntu) distroless?



- There's a correlation between size of the image and number of CVEs

# How and why (Ubuntu) distroless?



- There's a correlation between size of the image and number of CVEs
  - Reducing the size helps but isn't enough
  - Content provenance matters!
  - And Developer Experience + ecosystem + support also matters
- + reducing the size benefits both small and at-scale environments  
(reduces storage and memory resources consumption)

# How and why (Ubuntu) distroless?



Containers didn't kill Linux distributions....

... but ...

... there's a security and resources consumption challenge to solve

# How and why (Ubuntu) distroless?



- Google Distroless (<https://youtu.be/lviLZFciDv4>)

(+)

No package manager

No shell

About 20MB

Useful as/for runtime images

(-)

Complex to use

Complex to build

No support

Built with Bazel

The video player shows a presentation slide with the following content:

### State of “distroless” runtimes

- Early days...
  - Bootstrapping by selectively extracting debs.
- Growing Language Support
  - Go (gcr.io/distroless/base)
  - C++ / Rust / D (gcr.io/distroless/cc)
  - Java / Scala / Groovy (gcr.io/distroless/java/...)
  - Python (gcr.io/distroless/python2.7)
  - Node.js (gcr.io/distroless/nodejs)
- Requests, Issues, and PRs welcome.

The video player interface includes a progress bar at 26:07 / 32:24, a title '2017 swampUP Sessions | Distroless Docker: Containerizing Apps, not VMs - Matthew Moore', and engagement metrics: 18,986 views, Jul 11, 2017, 342 likes, and options for dislike, share, download, clip, and save.

# How and why (Ubuntu) distroless?



- Google Distroless (<https://youtu.be/lviLZFciDv4>)

(+)

No package manager

No shell

About 20MB

Useful as/for runtime images

(-)

Complex to use

Complex to build

No support

Built with Bazel

The video player shows a presentation slide with the following content:

### State of “distroless” runtimes

- Early days...
  - Bootstrapping by selectively extracting debs.
- Growing Language Support
  - Go (gcr.io/distroless/base)
  - C++ / Rust / D (gcr.io/distroless/cc)
  - Java / Scala / Groovy (gcr.io/distroless/java/...)
  - Python (gcr.io/distroless/python2.7)
  - Node.js (gcr.io/distroless/nodejs)
- Requests, Issues, and PRs welcome.

The video player interface includes a progress bar at 26:07 / 32:24, a title '2017 swampUP Sessions | Distroless Docker: Containerizing Apps, not VMs - Matthew Moore', and engagement metrics: 18,986 views, Jul 11, 2017, 342 likes, and options for dislike, share, download, clip, and save.



# How and why (Ubuntu) distroless?



Could we have the advantages of a Linux distribution


... without the overhead?

# How and why (Ubuntu) distroless?



- Chiselled Ubuntu containers for <insert-app-or-runtime>

Explore > [ubuntu/dotnet-deps](#)



## ubuntu/dotnet-deps

By [Canonical](#) • Updated 24 days ago

Chiselled Ubuntu for self-contained .NET & ASP.NET apps. Long-term tracks maintained by Canonical.

Image

VERIFIED PUBLISHER ☆


↓ Pulls 259

Overview **Tags**

Sort by Newest

TAG

[latest](#) ✓ Log4Shell CVE not detected  
Last pushed 2 days ago by [ccordeiro](#)

docker pull ubuntu/dotnet-deps:latest 

DIGEST	OS/ARCH	COMPRESSED SIZE
<a href="#">9baadf584c</a>	linux/amd64	5.3 MB
<a href="#">564f3d4a16cc</a>	linux/arm64/v8	4.19 MB
<a href="#">1c80b72db6d0</a>	linux/ppc64le	5.52 MB
<a href="#">1505e7607070</a>	linux/s390x	4.15 MB

# Chiselled Ubuntu containers?



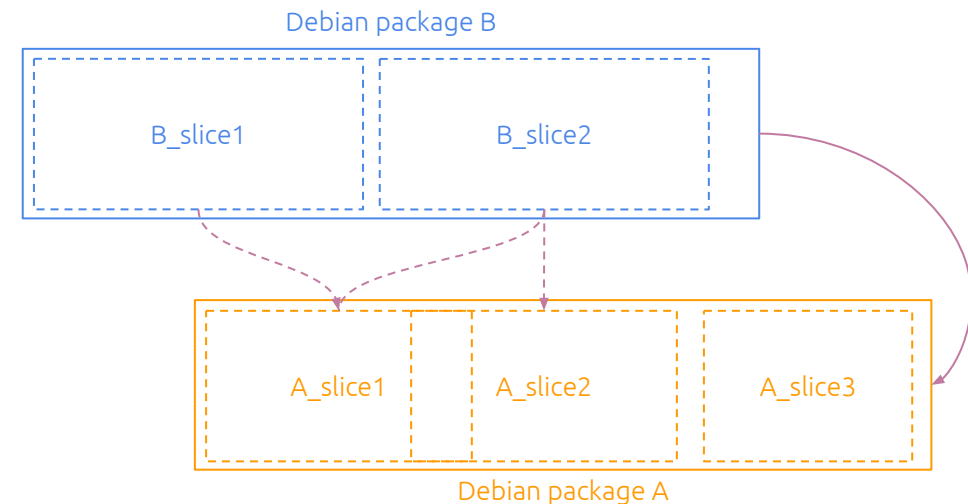
- <12MB for an “Ubuntu Distroless base”
- No package manager (avoid whole class of attacks)
- No shell (avoid whole class of attacks)
- Based on known and supported Ubuntu packages
- Compatible developer experience from host/server/container/chiselled

- *from (70MB, build)*

FROM ubuntu:22.04

*to (13MB, run)*

FROM ubuntu/dotnet-deps:22.04



# Questions / Comments

