CONTAINERS:

UNDER THE HOOD

Vincent Batts @vbatts

```
$> finger $(whoami)
Login: vbatts                              Name: Vincent Batt
Directory: /home/vbatts                    Shell: /bin/bash
Such mail.
Plan:
OHMAN
```

OPEN CONTAINER INITIATIVE

OPENSHIFT origin

PROJECT ATOMIC

HANDS-ON:

- capabilities
- Syscalls
- Namespaces
- Copy-On-Write (CoW)
- Archives

p.s. Don't forget to fill out the surveys!

SO,

WHY, CONTAINERS?

SO,
WHY, CONTAINERS?

Single Application

SO,
WHY, CONTAINERS?

```
Single Application
    Full System
```

SO,
WHY, CONTAINERS?

Single Application

Full System

But Not a VM

SO,
WHY, CONTAINERS?

```
Single Application
     Full System
         But Not a VM
             Except Maybe a VM
```

SO,
WHY, CONTAINERS?

Single Application

Full System

But Not a VM

Except Maybe a VM

Pods of applications

SO,
WHY, CONTAINERS?

- Single Application
  - Full System
    - But Not a VM
      - Except Maybe a VM
    - Pods of applications
  - Labels of services

SO,
WHY, CONTAINERS?

- Single Application
  - Full System
    - But Not a VM
      - Except Maybe a VM
    - Pods of applications
  - Labels of services
- Non-root

SO,
WHY, CONTAINERS?

- Single Application
  - Full System
    - But Not a VM
      - Except Maybe a VM
    - Pods of applications
  - Labels of services
- Non-root
  - Desktop Applications

SO,
WHY, CONTAINERS?

- Single Application
  - Full System
    - But Not a VM
      - Except Maybe a VM
    - Pods of applications
  - Labels of services
- Non-root
  - Desktop Applications
    - OMG AND CATS

SO,
WHY, CONTAINERS?

- Single Application
    - Full System
        - But Not a VM
            - Except Maybe a VM
        - Pods of applications
    - Labels of services
- Non-root
    - Desktop Applications
        - OMG AND CATS

https://www.flickr.com/photos/27549668@N03/

But Wait,

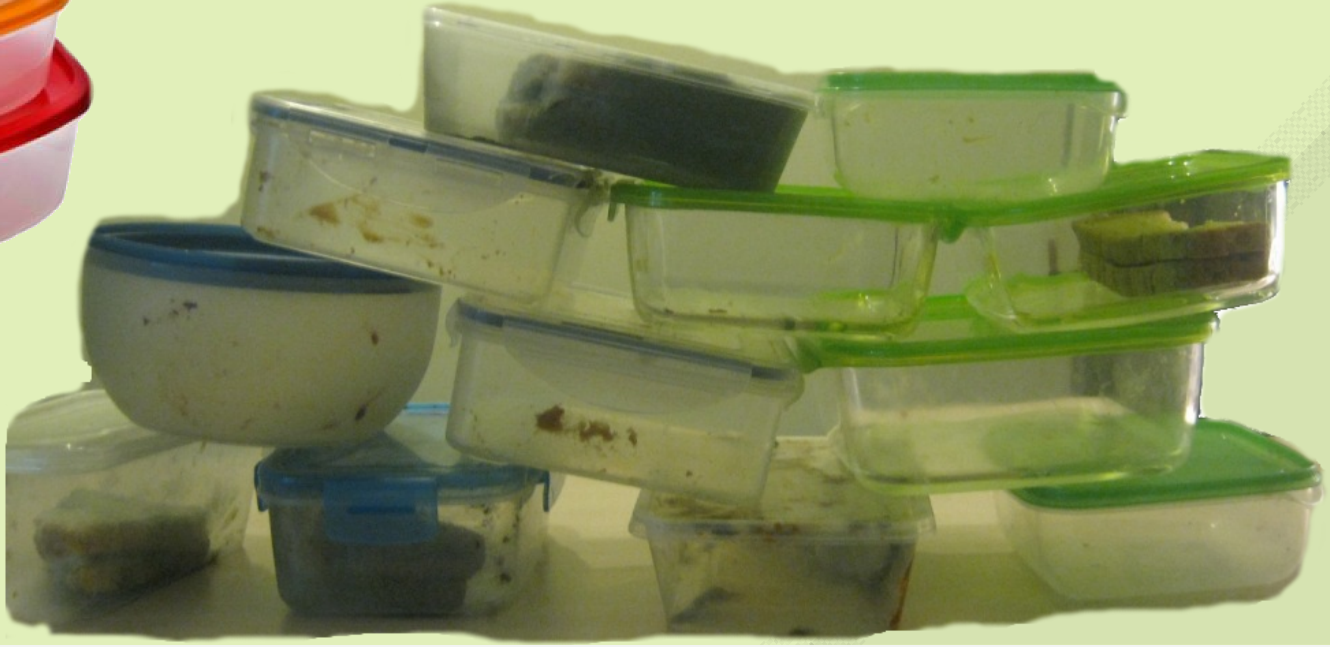
What does "container" mean to you?

But Wait,

What does "container" mean to you?

But Wait,

What does "container" mean to you?



CAPABILITIES

- capabilities(7)
- setpriv(1) (only on some versions of util-linux)
- capsh(1)
- proc(5)

CAPABILITIES

- capabilities(7)
- setpriv(1) (only on some versions of util-linux)
- capsh(1)
- proc(5)

DEMO

GOOD IDEA:

GOOD IDEA:

whistling while you work

GOOD IDEA:

whistling while you work

BAD IDEA:

GOOD IDEA:

whistling while you work

BAD IDEA:

whistling while you eat

SYSCALLS

- seccomp(2)
- proc(5)

SYSCALLS

- seccomp(2)
- proc(5)

DEMO

GOOD IDEA:

GOOD IDEA:

feeding a stray kitten in the park

GOOD IDEA:

feeding a stray kitten in the park

BAD IDEA:

GOOD IDEA:

feeding a stray kitten in the park

BAD IDEA:

feeding a stray kitten in the park to a bear

NAMESPACES

- unshare(1)
- proc(5)
- lsns(8)
- nsenter(1)

NAMESPACES

- unshare(1)
- proc(5)
- lsns(8)
- nsenter(1)

DEMO

GOOD IDEA:

GOOD IDEA:

playing catch with your grandpa

GOOD IDEA:

playing catch with your grandpa

BAD IDEA:

GOOD IDEA:

playing catch with your grandpa

BAD IDEA:

playing catch ***with*** your grandpa

COPY-ON-WRITE (COW)

- lvmthin(7)
- btrfs-subvolume(8)
- overlayFS

COPY-ON-WRITE (COW)

- lvmthin(7)
- btrfs-subvolume(8)
- overlayFS

DEMO

GOOD IDEA:

GOOD IDEA:

being served breakfast in bed

GOOD IDEA:

being served breakfast in bed

BAD IDEA:

GOOD IDEA:

being served breakfast in bed

BAD IDEA:

being served tennis balls in bed

FS *MAGIC*

shared subtree propogation

GOOD IDEA:

GOOD IDEA:

ordering a chili dog to go

GOOD IDEA:

ordering a chili dog to go

BAD IDEA:

GOOD IDEA:

ordering a chili dog to go

BAD IDEA:

ordering a chili dog that makes you go

TAR ARCHIVES

- format
- tar-split

GOOD IDEA:

GOOD IDEA:

Dressing up at Halloween as a pirate

GOOD IDEA:

Dressing up at Halloween as a pirate

BAD IDEA:

GOOD IDEA:

Dressing up at Halloween as a pirate

BAD IDEA:

Dressing up at Halloween as a piñata

VINCENT BATTS

@VBATTS| VBATTS@REDHAT.COM

THANKS!